



ORiNOCO AP-2500

User Guide



Take your network further

Copyright

© 2003 Proxim Corporation. All rights reserved. Covered by one or more of the following U.S. patents: 5,231,634; 5,875,179; 6,006,090; 5,809,060; 6,075,812; 5,077,753. This user's guide and the software described in it are copyrighted with all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of Proxim Corporation.

Trademarks

ORINOCO is a registered trademark, and Proxim and the Proxim logo are trademarks of Proxim Corporation. All other trademarks mentioned herein are the property of their respective owners.

Document Conventions

- The names of tabs, buttons, and fields appear in **Bold**.
- Screen names appear in ***Bold Italics***.
- To conserve space, sequential button or tab clicks are written as **Button 1 > Button 2**.
 - For example, **Configure > Network > DNS Server**, means:
 1. Click the **Configure** button.
 2. Click the **Network** tab.
 3. Click the **DNS Server** sub-tab.
- The term **USG** is synonymous with **AP** or **Access Point** and refers to the AP-2500.

Notes and Cautions



NOTE

A Note indicates important information that helps you make better use of your computer.



CAUTION

A Caution indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.



NOTE

Remember to review the contents of this manual, especially sections on information you need, before performing an operation.

Contents

1	Introduction	13
	Introducing the AP-2500	13
	Overview of Product Features	13
	Public Space Features	13
	Dynamic Address Translation (DAT)	14
	Networking Features	16
	IEEE 802.11 Specifications	16
	802.11a and 802.11b Networks	17
	Limitations on Roaming	17
	List of Networking Features	18
	The Product Package	20
	Minimum System Requirements	20
	Management and Monitoring Capabilities	20
	Web Browser Interface	21
	Command Line Interface	21
	SNMP Management	21
	Wireless Network Manager	22
	Active Ethernet	22
2	Installation & Basic Configuration	23
	Prerequisites	23
	Hardware Installation	24
	AP-2500 with Active Ethernet	24
	AP-2500 with Power Supply	26
	Installing a Card in Slot B	28
	5 GHz Kit Installation	28
	Installing the AP-2500 in a Plenum	30
	Initialization (ScanTool)	31
	ScanTool Instructions	31
	Basic Configuration	33
	Logging into the Web Interface	33
	Set System Name, Location and Contact Information	35
	Set the Access Point's IP Address	35

Contents

Configure Network Names for the Wireless Interfaces	36
Configure the Ethernet Interface	37
Set WEP Encryption for each Wireless Interface	37
Set and Change Passwords	38
Configure the Date and Time	39
Configuring the Date/Time Using NTP	39
Configuring the Date/Time Manually	39
Reboot the AP	40
Download the Latest Software	40
Setup your TFTP Server	40
Download Updates from your TFTP Server using the Web Interface	40
Download Updates from your TFTP Server using the CLI Interface	41
Back-up the AP's Configuration Files	41
Uploading Configuration Files	41
Downloading Configuration Files	42
3 AP-2500 Authentication Methods	43
Authentication Overview	43
Internal Authentication	44
End User Experience	45
Configuration Instructions	45
Internal Authentication with RADIUS	51
Authentication Procedure	51
Notes Concerning RADIUS	52
Configuration Instructions	52
Install and Configure RADIUS	52
Configure the AP-2500	55
External Authentication	58
Authentication Procedure	58
Configuration Instructions	59
Setup your External Web Server	59
Configure the AP-2500	59
4 Network Parameters	62
System	62
Network	63
IP Configuration	63
DHCP Server	63
Overview of DHCP Server Parameters	64
Configuring the AP to Serve Public IP Addresses	65

Contents

Disabling the AP's DHCP Server	65
IP Upsell	66
DNS Server	68
VLAN	69
Typical VLAN Configurations	69
VLAN Workgroups and Traffic Management	70
Traffic Management	70
Typical User VLAN Configurations	70
Setting Up Independent VLAN Workgroups	70
Setting Up Independent VLAN Workgroups	71
Setting Up a Single VLAN Workgroup	72
Interfaces	73
Wireless (802.11a)	74
Dynamic Frequency Selection (DFS)	75
RTS/CTS Medium Reservation	75
Wireless (802.11b)	75
Distance Between APs	77
Multicast Rate	78
Wireless Distribution System (WDS)	79
Ethernet	81
Management	81
Passwords	81
IP Access Table	82
Services	82
Network Time Protocol (NTP)	84
Filtering	84
Ethernet Protocol	84
Static MAC	85
Alarms	87
Groups	87
Alarm Host Table	87
Bridge	88
Security	88
MAC Access	88
Subscribers and MAC Access Control	89
RADIUS	90
RADIUS Overview	90
Unique AP-2500 RADIUS Client Features	90
RADIUS Messages and RADIUS Attributes	91
Sample RADIUS Transmissions	94
RADIUS Configuration Parameters	96

Contents

Encryption	99
VPN	99
Special Considerations Regarding VPN Support	100
5 Public Space Parameters	101
Home Page Redirection (HPR)	102
Authentication, Authorization, and Accounting (AAA)	103
AAA Basic	103
AAA Services with an External Web Server (EWS).	104
AAA Services with the Internal Web Server (IWS)	105
Secure Socket Layer (SSL)	105
Portal Page.	108
Smart Client	117
User Name & New Subscribers	119
Credit Card Services	120
Logging	125
General Syslog Information	125
Configuration Instructions	126
Sample Logging Events.	127
URL Filtering	131
URL Filtering by DNS Names	131
URL Filtering by IP Address	132
Information and Control Console (ICC)	132
ICC Appearance	133
Customizing the ICC	134
Potential End User Issues	137
SMTP Redirection	137
Passthrough Addresses	138
Passthrough DNS Table	139
Passthrough IP Table.	140
Passthrough AAA Port.	140
Bandwidth Management	140
Billing Options for Subscribers	142
Creating a Free Billing Plan	145
Subscriber Messages	146
Enabling Cookie Support.	150
Changing the Login Screen Logos	151

Contents

Authorized Subscribers	153
Authorized Subscribers Table and the Current Subscribers Table	154
Manually Adding a Subscriber	154
Removing a Subscriber	155
6 Monitor Information	156
System Status	157
Version	158
ICMP	159
IP/ARP Table	160
Learn Table	161
Current Subscribers Table	162
DAT Sessions	163
Interfaces	164
Link Test (802.11b Only)	165
7 Commands	167
Download	167
File Type Overview	168
Download Instructions	168
Upload	169
Reboot	170
Reset	170
Help Link	171
8 Troubleshooting	172
Troubleshooting Concepts	173
Symptoms and Solutions	173
Connectivity Issues	173
AP-2500 Unit Will Not Boot - No LED Activity	173
Serial Link Does Not Work	173
Ethernet Link Does Not Work	174
Basic Software Setup and Configuration Problems	174
Lost AP-2500, Telnet, or SNMP Password	174
Client Computer Cannot Connect	174
AP-2500 Has Incorrect IP Address	174
HTTP (browser) or Telnet Interface Does Not Work	174
HTML Help Files Do Not Appear	175
Telnet CLI Does Not Work	175
TFTP Server Does Not Work	175

Contents

Client Connection Problems	175
Client Manager Finds No Connection.	175
Client PC Card Does Not Work	175
Intermittent Loss of Connection	175
Client Does Not Receive an IP Address - Cannot Connect to Internet	175
VLAN Operation Issues	176
Verifying Proper Operation of the VLAN Feature	176
VLAN Workgroups	176
Active Ethernet	176
The AP-2500 Unit Does Not Work	176
There Is No Data Link.	176
“Overload” Indications	176
Recovery Procedures	177
Reset to Factory Default Procedure	177
Forced Reload Procedure	177
Download a New Image Using ScanTool	177
Download a New Image Using the Bootloader CLI	178
Setting IP Address using Serial Port and Normal CLI	180
Hardware and Software Requirements.	180
Attaching the Serial Port Cable.	180
Initializing the IP Address using Normal CLI	180
System Alarms (Traps)	181
Security Alarms	181
Wireless Interface Card Alarms.	181
Operational Alarms	181
FLASH Memory Alarms.	181
TFTP Alarms	181
Image Alarms.	182
Standard MIB-II (RFC 1213) Alarms	182
AAA Alarms	182
Related Applications	182
RADIUS Server	182
TFTP Server	182
LED Indicators	183
A Using the Command Line Interface	184
Prerequisite Skills and Knowledge	185
Notation Conventions	185
Important Terminology	185
Navigation and Special Keys	185
CLI Error Messages.	186

Contents

Command Line Interface (CLI) Variations	186
Bootloader CLI	186
CLI Command Types	187
Operational CLI Commands	187
? (List Commands)	188
done, exit, quit	190
download	190
help	190
history	191
passwd	191
reboot	191
search	192
upload	192
Parameter Control Commands	193
“set” and “show” Command Examples	193
Using Tables & User Strings	195
Working with Tables	195
Using Strings	196
Configuring Objects that Require Reboot	197
“set” CLI Command	197
“show” CLI Command	197
Configuring the AP-2500 Unit using CLI commands	198
Log Into the AP-2500 Unit using HyperTerminal	198
Log Into the AP-2500 Unit using Telnet	198
Set Basic Configuration Parameters using CLI Commands	198
Set System Name, Location and Contact Information	198
Set Static IP Address for the AP-2500 device	199
Set a Network Name for each Wireless Interface	199
Set WEP Encryption for each Wireless Interface	200
Change Passwords	201
Other Network Settings	201
VLAN Management	201
Add Entry to VLAN ID Table	201
Change your Wireless Interface Settings	202
Enable/Disable Interference Robustness	202
Enable/Disable Closed System	202
Enable/Disable Load Balancing	202
Enable/Disable Medium Density Distribution	202
Autochannel Select (ACS)	202
Set the Distance Between APs	202

Contents

Set the Multicast Rate	203
Set Ethernet Speed and Transmission Mode	203
Set Interface Management Services	203
Set Communication Ports	203
Set Session Timeouts	203
Configure Management Ports	204
Edit IP Access Table	204
Configure Serial Port Interface	204
Parameter Tables	205
System Parameters	206
Miscellaneous System Parameters	206
Inventory Management Information	207
Network Parameters	207
Location Parameters	207
DHCP Server Parameters	208
DNS Parameters	208
VLAN Parameters	209
Interface Parameters	209
Wireless 802.11b Parameters	209
Wireless 802.11a Parameters	211
Ethernet Interface Parameters	212
Management Parameters	212
IP Access Table Parameters	212
Access Control Parameters	212
SNMP Parameters	213
SNMP Table Host Table Parameters	213
Telnet Parameters	213
Serial Port Parameters	214
HTTP (web browser) Parameters	214
TFTP Server Parameters	214
NTP Parameters	215
Security Parameters	216
RADIUS Server Parameters	216
Encryption Parameters	218
VPN	218
Home Page Redirection Parameters	218
AAA Parameters	219
Basic AAA Parameters	219
AAA External Authorization Parameters	219
AAA Internal Authorization Parameters	220
Logging Parameters	220

Contents

URL Filtering Parameters	221
URL Filtering IP Table	221
URL Filtering DNS Table	221
ICC (Information Control Console) Parameters	222
ICC Button Configuration	222
ICC Banner Configuration	223
SMTP Parameters	223
Passthrough Parameters	223
Passthrough IP Table	224
Passthrough DNS Table	224
AAA Passthrough Port	224
Bandwidth Management Parameters	224
Billing Parameters	225
Billing Mirroring Parameters	225
Billing Plans Configuration	226
Subscriber Messages Parameters	227
Authorized Subscribers Table	229
Current Subscribers Table	230
Miscellaneous Parameters	231
CLI Monitoring Parameters	231
B XML Interface Specification	232
AP-2500 XML Communication Overview	232
URL GET	233
XML POST	233
XML Query String Command Format	233
XML Response Form Format	234
Response Form Error Codes	234
AP Command Reference	235
Add/Update User	235
Update Cache	235
Bandwidth Up	236
Bandwidth Down	236
Delete User	236
Query User	237
Authorize User	237
Commands For Reference Only	238
Set Room Access	238
Query Room Status	238
User Purchase	238
User Payment	239

External Authentication Procedure (Detailed)	240
Sample XML Communications with the AP	241
C Credit Card Interface Specification	242
Data sent by the AP-2500 to the credit card clearing server	242
Data sent by credit card clearing server to the AP-2500	243
Explanation:	243
D ASCII Character Chart	244
E Specifications	245
Hardware Specifications	245
Physical Specifications	245
Electrical Specifications	245
Environmental Specifications	245
Ethernet Interface	246
PCMCIA Interface	246
Serial Port Interface	246
Active Ethernet Interface	246
HTTP Interface	246
Radio Specifications	247
802.11b Channel Frequencies	247
802.11a Channel Frequencies	247
Wireless Communication Range	248
F Technical Support	249

Introduction

In This Chapter

- [Introducing the AP-2500](#)
- [Overview of Product Features](#)
- [The Product Package](#)
- [Minimum System Requirements](#)
- [Management and Monitoring Capabilities](#)
- [Active Ethernet](#)

Introducing the AP-2500

The ORiNOCO AP-2500 is an all-in-one wireless access point and access gateway specifically designed for public hotspot providers and enterprises. It is a cost-effective solution for small and medium public hotspots, such as coffee shops, hotels, and airport lounges, and it enables enterprises to offer corporate visitors immediate wireless network access regardless of their existing network or ISP settings. Supporting Wi-Fi 802.11b and 802.11a it ensures ease-of-use and secure Internet access for mobile professionals. Each AP supports a maximum of 50 subscribers. Advanced features include Radius AAA, VPN passthrough, dynamic address translation, home page redirect, internal web server, walled garden, bandwidth management, and remote management providing service differentiation and operating cost savings for hotspot operators. The AP-2500 is a true Hotspot-in-a-box solution.

Overview of Product Features

The AP-2500 supports two feature sets:

1. Access gateway or Public Space features (that provide hotspot connectivity)
2. Standard networking features included with many traditional wireless access points (such as the ORiNOCO AP-2000)

Although in implementation there is some overlap between these feature sets, for the sake of simplicity this document refers to the first set of features as the AP's **Public Space** features and the second set as the AP's **Networking** features.

Public Space Features

The AP-2500's Public Space features are designed to provide a simple billing, management, and authentication solution for hotspot operators and quick and easy access to the Internet for subscribers. Subscribers do not need to change any settings (such as IP address or Internet proxy server configuration) on their computer to connect to the hotspot.

Noteworthy Public Space features include:

- **Dynamic Address Translation:** The AP-2500 offers plug-and-play connectivity for subscribers without any intervention required on the part of the subscriber. The AP-2500 supports all possible IP settings (static addressing, dynamic addressing, static DNS server settings). A subscriber simply turns on his/her laptop and launches a Web browser to connect to the Internet. See [Dynamic Address Translation \(DAT\)](#) for details.
- **Transparent Proxy Redirection:** The AP directs all HTTP and HTTPS proxy requests through an internal proxy which is transparent to the subscriber. In other words, your subscribers don't have to change their browser' proxy settings (if enabled).

Introduction

- **Outgoing e-mail (SMTP) Redirection:** You can configure the AP-2500 to redirect outgoing e-mail messages to a specified Simple Mail Transfer Protocol (SMTP) server. Subscribers can send e-mails as if they were connected to their home network. See [SMTP Redirection](#) for details.
- **VPN Passthrough:** The AP-2500 can support multiple PPTP and IPsec VPN sessions for subscribers. See [VPN](#) for details.
- **Support for Application Level Gateways (ALGs):** The AP-2500 supports Application Level Gateways (ALGs) providing transparent access to subscribers for popular Web-based applications that do not work in typical Network Address Translation (NAT) environments (see [Dynamic Address Translation \(DAT\)](#) for details). The AP provides support for the following protocols:
 - H323 (protocol used by Microsoft NetMeeting)
 - Real Audio
 - SMTP
 - FTP
 - PPTP (for VPN connections)
 - IPsec (for VPN connections)
- **Multiple Authentication Options:** To authenticate subscribers, you can use the Access Point's Internal Web Server (IWS), an External Web Server (EWS), or RADIUS. See [AP-2500 Authentication Methods](#) for details.
- **SSL Support:** If using Internal authentication, you can copy your company's digital certificates to the AP-2500 to create HTTPS pages that provide end-to-end encrypted links between the AP and subscribers. See [Secure Socket Layer \(SSL\)](#) for details.
- **"Remember My Login" Cookie:** The Access Point can store a cookie in your subscriber's Web browser to facilitate future logins by the customer.
- **Billing Records Mirroring:** Access Points can send copies of credit card billing records to a list of external servers that you specify. See [Credit Card Mirroring](#) for details.
- **Information and Control Console:** The AP can open a Java pop-up window on your subscribers' Web browsers that reports the amount of time remaining in the user's account (if paid for by credit card) or allows the user to logout (if using RADIUS to manage users). Also, the ICC supports multiple advertising banners that you can customize for your hotspot. See [Information and Control Console \(ICC\)](#) for details.
- **Dynamic Billing Selection/Bandwidth Management:** With ICC enabled, subscribers can dynamically switch between billing plans to increase or decrease their own bandwidth.
- **Walled Garden:** You can provide unauthenticated users with free access to a limited number of Web sites as a promotional tool. See [Passthrough Addresses](#) for details.
- **Home Page Redirection:** You can automatically redirect subscribers to the Web site of your choice either before authentication (see [Portal Page](#)) and/or after authentication (see [Home Page Redirection \(HPR\)](#)).
- **IP Upsell:** You can configure the AP-2500 to offer public addresses to power users at a premium price. See [IP Upsell](#) for details.
- **URL Filtering:** You can prohibit your subscribers from accessing specific Web sites. See [URL Filtering](#) for details.

Dynamic Address Translation (DAT)

Dynamic Address Translation (DAT) is a technique that eliminates IP configuration issues and the associated complaints and support requests from subscribers.

Without DAT, a subscriber will typically need to change the following settings (twice -- once to join the hotspot network and then set them back again to rejoin the user's home network):

- IP Address
- Subnet Mask
- Default Gateway Address
- DNS Server Addresses
- Web browser's proxy settings
- Outgoing mail server settings

DAT eliminates the need for subscribers to change any of these settings. The AP-2500 automatically redirects subscriber messages to the appropriate location. DAT even works if a user's wireless card is configured with static IP settings.

Introduction

One of the key features of DAT is a technique known as **Network Address Translation (NAT)**. NAT is an Internet standard that allows a device (like the AP-2500) to use a single public IP address to provide Internet connectivity to multiple devices (which would otherwise each need to have its own public IP address to communicate with the network). The AP-2500 uses NAT for clients that are configured to obtain an IP address automatically from a DHCP server (which is the typical configuration for hotspot users) and for clients with “misconfigured” static IP addresses (that is, addresses that are not valid on the AP’s local IP network).

When performing NAT, an AP-2500 uses two IP addresses. One IP address is assigned by your ISP and is valid on the Internet. This is known as a **public** or **routable** IP address. In the illustration below, the AP is assigned a public IP address of 205.23.45.12.

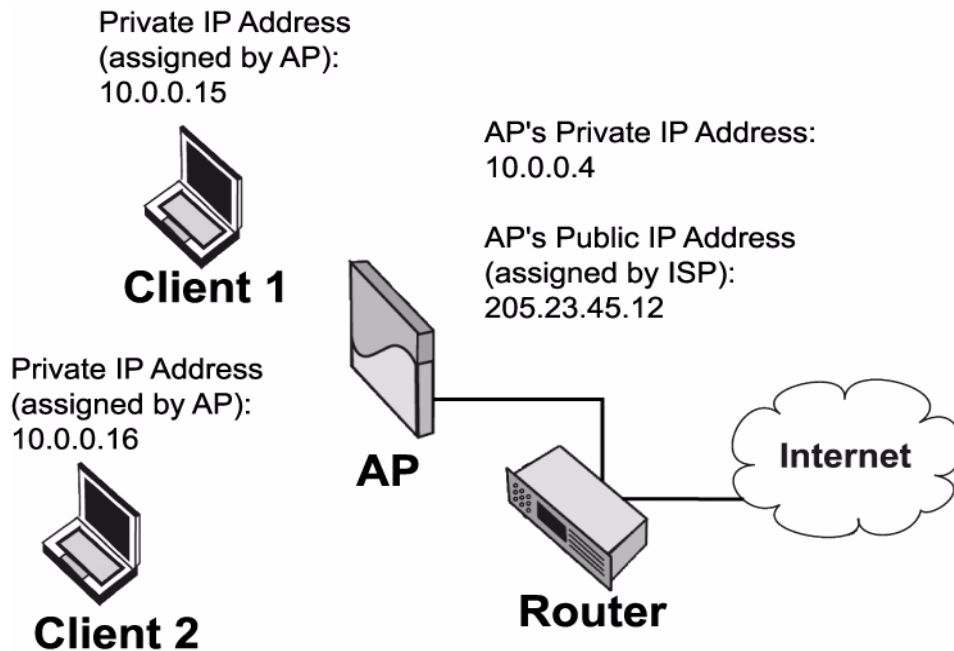


Figure 1-1 The AP-2500 and NAT

The second IP address assigned to the AP is its **private** IP Address. This address is not valid on the Internet. The Internet community has reserved several address ranges for private networks, including 10.0.0.0 and 192.168.0.0. By default, the AP assigns itself a private IP address of 10.0.0.4. It also acts as a DHCP server to assign IP address in that same private IP range to wireless subscribers. As shown in the illustration, the AP has assigned one client an IP address of 10.0.0.15 and a second client an IP address of 10.0.0.16.

When the AP receives traffic from Client 1, it modifies the packet header so Client 1’s private IP address (10.0.0.15) becomes the AP’s public IP address (205.23.45.12). Likewise, the AP performs the same function for traffic from Client 2.

The AP differentiates between its clients by specifying different UDP and TCP port numbers for traffic that originates from different clients. When the AP receives traffic from the Internet, the AP can determine to which client the traffic is intended based on the port numbers in use.

The NAT technique used by the AP-2500 is known by many names including **many-to-one NAT** (that is, many private IP addresses mapped to one public IP address) and **Network Address Port Translation (NAPT)** (due to the AP’s use of port numbers to differentiate clients). For more information on NAT, see RFC 3022 at <http://www.rfc-editor.org/>.

Introduction

Networking Features

The AP-2500 provides wireless access to the Internet for hotspot subscribers. This means that your customers can surf the Internet and send e-mails from anywhere within range of the Access Point without having to install extra wires or cabling.

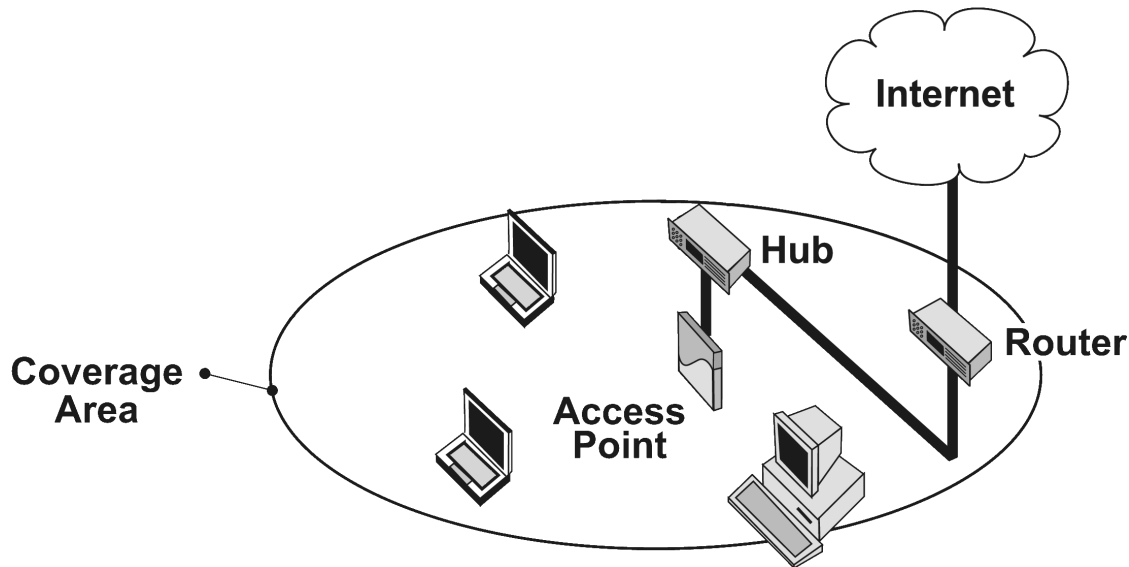


Figure 1-2 Sample AP-2500 Hotspot Configuration

The AP-2500 supports the full set of wireless networking features that are typically available with traditional access points (that is, access points that do not supply hotspot connectivity), including:

- Easy installation and operation
- Over-the-air encryption of data
- High speed network links
- Support for multiple IEEE standards

IEEE 802.11 Specifications

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) adopted the 802.11 standard for wireless devices operating in the 2.4 GHz frequency band. This standard includes provisions for three radio technologies: direct sequence spread spectrum, frequency hopping spread spectrum, and infrared. Devices that comply with the 802.11 standard operate at a data rate of either 1 or 2 Megabits per second (Mbps/sec).

In 1999, the IEEE modified the 802.11 standard to support direct sequence devices that can operate at speeds of up to 11 Mbps/sec. The IEEE ratified this standard as **802.11b**. 802.11b devices are backwards compatible with 2.4 GHz 802.11 direct sequence devices (that operate at 1 or 2 Mbps/sec).

Also in 1999, the IEEE modified the 802.11 standard to support devices operating in the 5 GHz frequency band. This standard is referred to as **802.11a**. 802.11a devices are not compatible with 2.4 GHz 802.11 or 802.11b devices. 802.11a radios use a radio technology called Orthogonal Frequency Division Multiplexing (OFDM) to achieve data rates of up to 54 Mbps/sec.

Introduction

802.11a and 802.11b Networks

The AP-2500 supports both the IEEE 802.11a and 802.11b standards. The AP-2500 can be used with the following combinations of 802.11a and 802.11b radio cards:

- One 802.11b card (second slot empty)
- One 802.11a 5 GHz upgrade kit (second slot empty)
- Two 802.11b cards
- One 802.11b card and one 802.11a 5 GHz upgrade kit

You can have an 802.11a and an 802.11b card present in the AP-2500 at the same time and 2.4 GHz and 5 GHz clients will be supported simultaneously.

The coverage area achieved with a 2.4 GHz radio is generally larger than that of a 5 GHz radio (this is particularly true for open spaces but less so for indoor applications). The transmit rate is higher in the smaller (5 GHz) cell than the larger (2.4 GHz cell). The following diagram illustrates the difference in cell sizes. However, the best way to determine the AP-2500's actual coverage area is to test the range of a wireless connection using a client device.

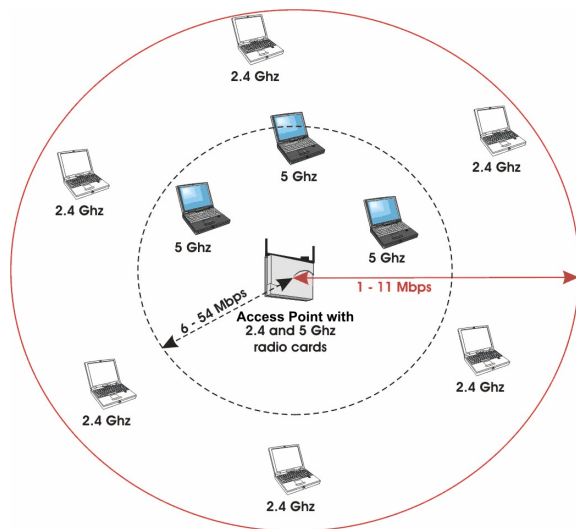


Figure 1-3 802.11a versus 802.11b Coverage Area

Limitations on Roaming

Roaming is the ability of a wireless client to move from one Access Point to another while maintaining an uninterrupted connection to the network. Most traditional Access Points support this feature. While the AP-2500 supports seamless roaming from a radio perspective, in practice it does not support seamless roaming for subscribers from AP-2500 to AP-2500 in a hotspot environment. Each AP-2500 maintains its own list of current subscribers that can access the Internet; this list is not shared between AP-2500s.

Limited roaming can be achieved under the following circumstances:

1. A subscriber can seamlessly roam between two radios installed in the AP-2500. For example, a subscriber with an 802.11b client can roam between the Access Point's two 802.11b cells when two 802.11b cards are installed. (This assumes that the two cells have the same Network Name and Encryption settings.)
2. If you use a RADIUS server to authenticate subscribers, a subscriber can move between multiple AP-2500s but the user will need to re-login each time he connects to a different Access Point. This solution does not provide seamless roaming.



NOTE

If you have enabled the [Information and Control Console \(ICC\)](#), a RADIUS user who clicks the **Logout** button will not be logged out following a roam from one AP-2500 to another. The user will need to browse new pages to bring up the login screen for the new AP and re-login when prompted.

Introduction

List of Networking Features

The IEEE standards that governs wireless communications are different for the 2.4 GHz band and the 5 GHz band. The table below compares the software features supported for each type of card in the AP-2500 device:

Feature	2.4 GHz (802.11b)	5 GHz (802.11a)	Comments
Number of stations per BSS	up to 250	up to 50	This specifies the limits of each radio. Note that the AP-2500's Public Space features can support a maximum of 50 subscribers.
HTTP Server	yes	yes	
Telnet / CLI	yes	yes	
SNMP Agent	yes	yes	
VLAN Support (2 User VLANs)	yes	yes	
Emergency Reset to Default Configuration	yes	yes	
DHCP Client	yes	yes	
DHCP Server	yes	yes	
TFTP	yes	yes	
802.1d bridging	yes	yes	
MAC Access Control Table	yes	yes	
Ethernet Protocol Filtering	yes	yes	
ICMP Echo Response (i.e., responds to pings)	yes	yes	
Hardware Watchdog Timer	yes	yes	
Automatic Channel Select	yes	yes	
WEP	yes	yes	Key lengths supported: 64-bit and 128-bit (Note: Some products refer to 64-bit as "40-bit" and 128-bit as "104-bit". 128-bit encryption may not be available with all 802.11b cards.)
WEP Plus (Weak Key Avoidance)	yes	no	Available only one way (AP to client) if using an ORiNOCO 802.11a/b ComboCard or a non-ORiNOCO client.
WDS Relay	yes	no	
Remote Link Test	yes*	no	
Link Test Responder	yes*	no	
Medium Density Distribution	yes*	no	
Distance between APs	yes*	no	
Closed System	yes	no	
Interference Robustness	yes	no	
Load Balancing	yes	no	No client support for 802.11a
AP List	yes	no	No client support for 802.11a
SpectraLink VoIP Support	yes	no	
Fragmentation	yes	yes	For 802.11b, Fragmentation is implemented as part of the Interference Robustness feature.
Dynamic Frequency Selection (DFS)	no	yes	DFS is required for 802.11a products sold in Europe

*This feature is not available if you are using an ORiNOCO 802.11a/b ComboCard or a non-ORiNOCO client with 802.11b.

Introduction

The following table provides detailed information on the differences between the 802.11a and 802.11b feature sets.

	2.4 GHz (802.11b)	5 GHz (802.11a)
Physical Layer Type (Modulation Type)	DSSS (Direct Sequence Spread Spectrum)	OFDM (Orthogonal Frequency Division Multiplexing)
Auto Channel Select	enable (default) disable	enable (default) disable
Frequency Channel	1 - 2.412 GHz 2 - 2.417 GHz 3 - 2.422 GHz (default FCC, ETSI, Japan) 4 - 2.427 GHz 5 - 2.432 GHz 6 - 2.437 GHz 7 - 2.422 GHz 8 - 2.447 GHz 9 - 2.452 GHz 10 - 2.457 GHz 11 - 2.462 GHz 12 - 2.467 GHz (ETSI countries only) 13 - 2.472 GHz 14 - 2.477 GHz (Japan only) For France, channels 10-13 only	36 - 5.180 GHz 40 - 5.200 GHz 44 - 5.220 GHz 48 - 5.240 GHz 52 - 5.260 GHz (default) 56 - 5.280 GHz 60 - 5.300 GHz 64 - 5.320 GHz Channels 36-64 are valid for products in the FCC and ETSI regulatory domains. The following channels are available in Japan: 34 - 5.170 GHz (default) 38 - 5.190 GHz 42 - 5.210 GHz 46 - 5.230 GHz
Transmit Rate	N/A	0 - Auto Fallback (default) 6 Mbit/sec 9 Mbits/sec 12 Mbits/sec 18 Mbits/sec 24 Mbits/sec 36 Mbits/sec 48 Mbits/sec 54 Mbits/sec
Distance Between APs	large (default) medium small minicell microcell	N/A
Multicast Rate	1 Mbit/sec 2 Mbits/sec 5.5 Mbits/sec (default) 11 Mbits/sec Available options depend on Distance Between APs setting	0 - Auto Fallback (default) 6 Mbit/sec 9 Mbits/sec 12 Mbits/sec 18 Mbits/sec 24 Mbits/sec 36 Mbits/sec 48 Mbits/sec 54 Mbits/sec
Interference Robustness	enable (default) disable	N/A
Closed System	enable disable (default)	N/A
Load Balancing	enable (default) disable	N/A
Medium Density Distribution	enable (default) disable	N/A

Introduction

The Product Package

Each AP-2500 comes with the following:

- AP processor module
- AP cover
- Mounting plate
- Mounting hardware
 - Four 3.5 mm x 40 mm screws
 - Four 6 mm x 35 mm plugs
- One power supply (if you purchased the Power Supply model)
- One power cord (if you purchased the Power Supply model)
- One ORiNOCO Installation CD-ROM that contains the following:
 - Software Installation Wizard
 - ScanTool
 - Solarwinds TFTP software
 - HTML Help
 - this user's guide in PDF format
- One *Quick Start Guide*

If any of these items are missing or damaged, please contact your reseller or ORiNOCO Technical Support.



NOTE

PC Cards and/or 5 GHz upgrade kits are not included with your AP and must be ordered as separate items.

Minimum System Requirements

To begin using an AP-2500, you must have the following minimum requirements:

- A 10Base-T Ethernet or 100Base-TX Fast Ethernet switch or hub
- At least one radio card to insert into the AP (an 802.11b card or a 5 GHz upgrade kit)
- At least one wireless client that complies with the standard supported by the cards you intend to insert into the AP:
 - An 802.11a client device if you plan to install a 5 GHz upgrade kit
 - An 802.11b client device if you plan to insert one or more 802.11b radios in the AP
- An Ethernet computer that is connected to the same IP network as the AP-2500 and has one of the following Web browsers installed:
 - Microsoft Internet Explorer 5.5 or later (recommended)
 - Netscape 6 or later(The computer is required to configure the AP-2500 using the Web browser interface.)
- Internet connectivity on your Ethernet network

Management and Monitoring Capabilities

There are several management and monitoring interfaces available to the network administrator to configure and manage the AP-2500 on your network:

- [Web Browser Interface](#)
- [Command Line Interface](#)
- [SNMP Management](#)
- [Wireless Network Manager](#)



NOTE

For security reasons, you can only configure the AP-2500 over its Ethernet interface or serial port. You cannot configure the unit from a wireless client.

Introduction

Web Browser Interface

The Web Browser interface (also known as the HTTP interface) provides easy access to configuration settings and network statistics from any computer in the network. Use the Web browser interface through your LAN (switch, hub, etc.), over the Internet, or with a “crossover” Ethernet cable connected directly to your computer’s Ethernet Port.

Command Line Interface

The Command Line Interface (CLI) represents a set of keyboard commands and parameters used for configuring and managing the AP-2500.

Users enter Command Statements, composed of CLI Commands and their associated parameters. Statements may be issued from the keyboard for real time control, or from scripts that automate configuration.

For example, when downloading a file, administrators enter the **download** CLI Command along with IP Address, file name, and file type parameters.

- If necessary, use the CLI with your computer’s serial port to assign an IP address to your AP.
- The CLI provides configuration and management access for most generic Telnet and Terminal clients. Use the CLI through your computer serial port, over your LAN, over the Internet, or with a “crossover” Ethernet cable connected directly to your computer.

Details of the CLI commands used to manage the AP-2500 along with syntax and specific parameters names can be found in [Using the Command Line Interface](#).

SNMP Management

In addition to the Web and the CLI interfaces, you can also manage and configure an AP-2500 using the Simple Network Management Protocol (SNMP). Note that this requires an SNMP manager program, like HP Openview or Castlerock’s SNMPc.

The AP-2500 supports several Management Information Base (MIB) files that describe the parameters that can be viewed and/or configured over SNMP:

- MIB-II (RFC 1213)
- Ethernet-like MIB (RFC 1643)
- ORiNOCO Enterprise MIB
- Nomadix MIB (for Public Space and IP features)
- IEEE 802.11 MIB

Proxim provides these MIB files on the AP-2500 CD. You need to compile one or more of the above MIBs into your SNMP program’s database before you can manage the AP-2500. Refer to the documentation that came with your SNMP manager for instructions on how to compile MIBs.

The ORiNOCO and Nomadix MIB files define the read and read-write objects that can be viewed or configured using SNMP. These objects correspond to most of the settings and statistics that are available with the other management interfaces.

The ORiNOCO Enterprise MIB controls the following settings:

- All of the Networking parameters found under the **Configure** heading within the Web browser interface (described in [Network Parameters](#)), except for the following features:
 - [IP Configuration](#)
 - [DHCP Server](#)
 - [DNS Server](#)
 - [RADIUS](#)
 - [VPN](#)

Introduction

The Nomadix MIB controls the following settings:

- All of the Public Space features found under the **PublicSpace** and **Subscriber** headings within the Web browser interface (described in [Public Space Parameters](#)).
- The following Network parameters:
 - [IP Configuration](#)
 - [DHCP Server](#)
 - [DNS Server](#)
 - [RADIUS](#)
 - [VPN](#)

Refer to the MIB files for more information; the MIB files can be opened with any text editor, such as Microsoft Word or Notepad.



NOTE

The remainder of this guide describes how to configure an AP-2500 using the Web browser interface or the CLI interface. For information on how to manage devices using SNMP, refer to the documentation that came with your SNMP program. Also, refer to the MIB files for information on the parameters available via SNMP.

Wireless Network Manager

The Wireless Network Manager is Proxim's premier management tool for Access Points and Outdoor Routers. It provides a single management interface that lets an IT manager configure, manage, upgrade, and troubleshoot thousands of wireless devices from anywhere in the world. The Wireless Network Manager simplifies network maintenance and easily integrates in an existing SNMP management system.

See Proxim's Web site at <http://www.proxim.com/> for more information on the Wireless Network Manager.

Active Ethernet

Some AP-2500 units are equipped with an Active Ethernet module. Active Ethernet (AE) delivers both data and power to the access point over Ethernet cabling. There is no difference in operation; the only difference is in the power source.

- The Active Ethernet (AE) integrated module adds ~48 VDC to unused (non-data) wires in standard Category 5 Ethernet cable.
- The cable length between the Ethernet network source and the AP-2500 unit should not exceed 100 meters (approx 325 ft.). In other words, the length of cable connecting the Ethernet network to the power injector plus the length of the cable connecting the power injector to the AP cannot exceed 100 meters.
- The AE power injector is not a repeater and does not amplify the Ethernet data signal.
- AP-2500 devices without Active Ethernet should be connected to a grounding type AC outlet (100-240 VAC), using the standard power cord supplied.
- Output Power, per Port 11 Watts

Also see [Electrical Specifications](#).

2

Installation & Basic Configuration

In This Chapter

This chapter describes how to install the AP-2500 hardware and perform basic configuration operations.

- [Prerequisites](#)
- [Hardware Installation](#)
- [Initialization \(ScanTool\)](#)
- [Basic Configuration](#)
- [Download the Latest Software](#)
- [Back-up the AP's Configuration Files](#)

Prerequisites

Before installing an AP-2500, you need to gather certain network information. The following section identifies the information you need.

Network Name (SSID of the wireless cards)	You must assign the Access Point a Network Name before wireless users can communicate with it. The clients also need the same Network Name. This is not the same as the System Name, which applies only to the Access Point. The network administrator typically provides the Network Name.
AP-2500's IP Address	You will need to assign the Access Point an IP address that is valid on your network. While the Access Point can dynamically obtain an IP address, you may want to consider assigning it a static IP address that will not change. Some of the Public Access features will stop working if the AP's IP address changes after installation and configuration.
HTTP Password	Each Access Point requires a read/write password to access the web interface. The default password is "public".
CLI Password	Each Access Point requires a read/write password to access the CLI interface. The default password is "public".
SNMP Read Password	Each Access Point requires a password to allow get requests from an SNMP manager. The default password is "public".
SNMP Read-Write Password	Each Access Point requires a password to allow get and set requests from an SNMP manager. The default password is "public".
Security Settings	You need to determine what security features you will enable on the Access Point.
Authentication Method	You should decide which authentication method you plan to use before installing the Access Point: Internal Authentication, Internal Authentication with RADIUS, or External Authentication. See AP-2500 Authentication Methods for an overview of these options.
Client IP Address Pool Allocation Scheme	The Access Point will automatically provide IP addresses to subscribers as they sign on. You need to determine what range or ranges of IP addresses you want to offer. See DHCP Server for details.
DNS Server IP Address	The network administrator typically provides this IP Address. The Access Point needs to have properly configured DNS settings to function correctly.

Installation & Basic Configuration

Hardware Installation

Refer to the steps below that correspond to your configuration:

- [AP-2500 with Active Ethernet](#)
- [AP-2500 with Power Supply](#)
- [Installing a Card in Slot B](#)
- [5 GHz Kit Installation](#)
- [Installing the AP-2500 in a Plenum](#)

AP-2500 with Active Ethernet

Follow these installation steps if you purchased an AP with Active Ethernet:

1. Slide the AP module onto the mounting bracket. Make sure it is properly seated.

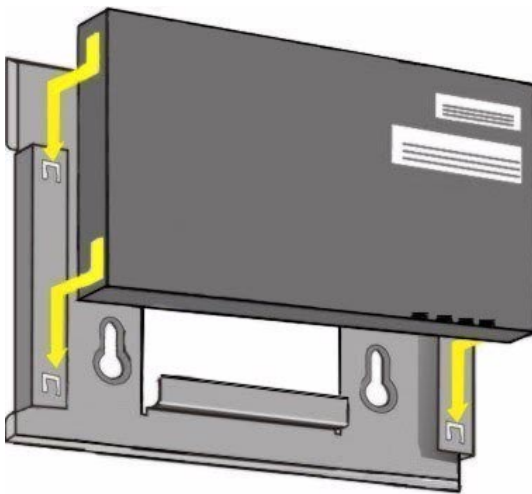


Figure 2-1 Insert Module into mounting bracket

2. Slide an 802.11b wireless card (not included in the kit) into Slot A.

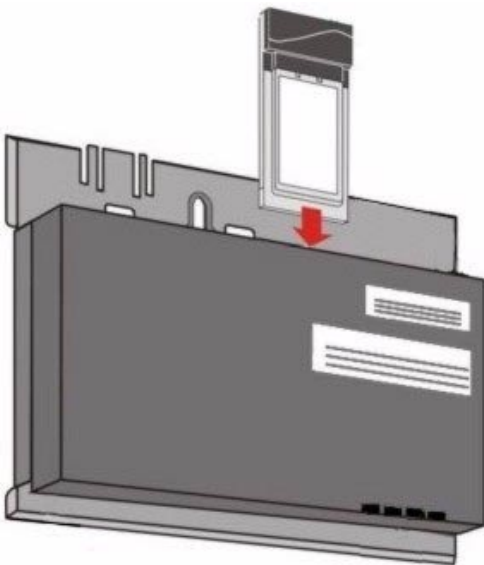


Figure 2-2 Slide a PC Card into the AP

Installation & Basic Configuration

➤ NOTE

If you want to install a second 802.11b wireless card in Slot B, you will first need to remove the slot cover (which is provided for plenum-rating purposes). See [Installing a Card in Slot B](#) for instructions. If you want to install a 5 GHz kit, see [5 GHz Kit Installation](#).

3. Connect one end of a Category 5 straight-through Ethernet cable to the Access Point's Ethernet port. The AP will receive both power and Ethernet connectivity over the cable.
4. Connect the other end of the cable to an Active Ethernet power injector (if not already connected).
5. Wait for the Power LED indicator to turn green before proceeding.

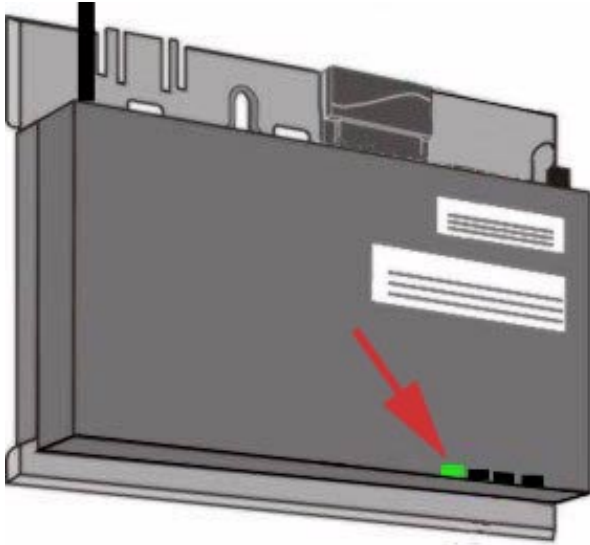


Figure 2-3 Connect an Ethernet cable from an AE hub to the AP

6. Determine the best location for your device.

➤ NOTE

Proxim recommends that you perform a Site Survey prior to determine the installation location for your AP-2500. For information about how to conduct a Site Survey, contact your local reseller.

7. Once you have chosen a final location for your unit, mount the wall bracket and the processor module and place the cover onto the unit as shown.

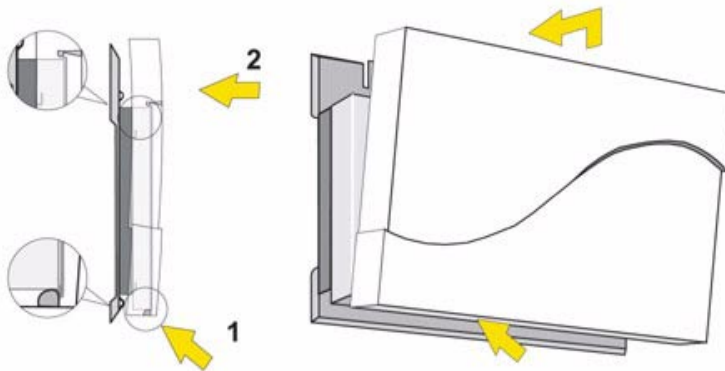


Figure 2-4 Wall mounting the AP

Installation & Basic Configuration

AP-2500 with Power Supply

Follow these installation steps if you purchased an AP with a power supply:

1. Clip the power supply into the mounting bracket.
2. Plug the AC power cord into the power supply.

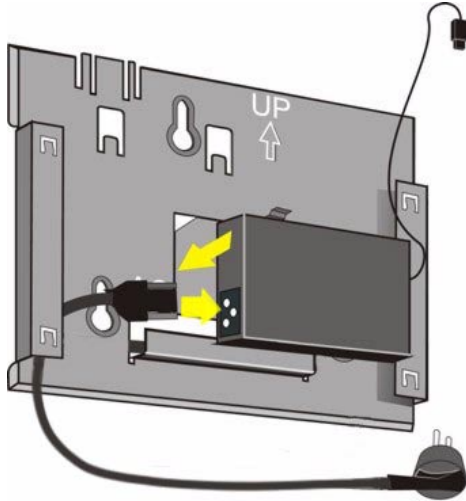


Figure 2-5 Install the power supply

3. Slide the AP module onto the mounting bracket. Make sure it is properly seated.
4. Plug the DC connector from the power supply into the top of the AP module.

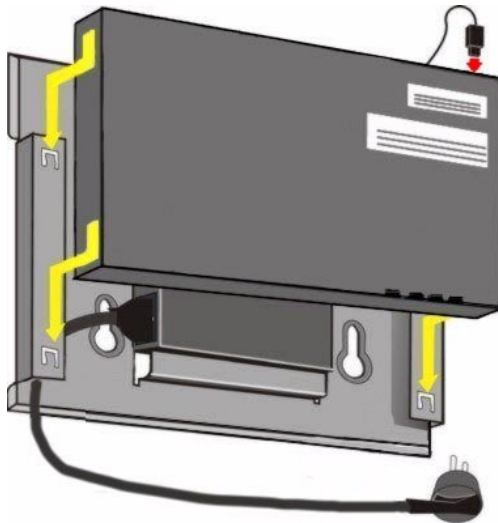


Figure 2-6 Insert module in mounting bracket and attach power connector

5. Slide an 802.11b wireless card (not included in the kit) into Slot A.

Installation & Basic Configuration

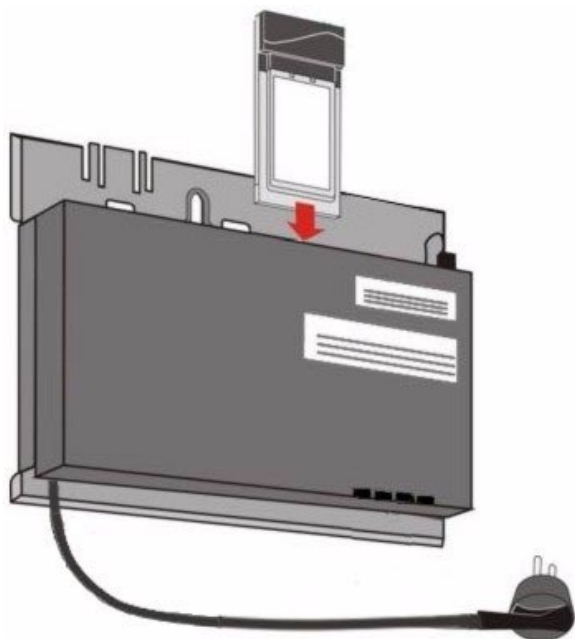


Figure 2-7 Slide a PC Card into the AP



NOTE

If you want to install a second 802.11b wireless card in Slot B, you will first need to remove the slot cover (which is provided for plenum-rating purposes). See [Installing a Card in Slot B](#) for instructions. If you want to install a 5 GHz kit, see [5 GHz Kit Installation](#).

6. Attach one end of an Ethernet cable to the AP's Ethernet port and the other end to a network hub or switch.
7. Connect the unit's power supply to a power source.
8. Wait for the power LED to turn green before proceeding.

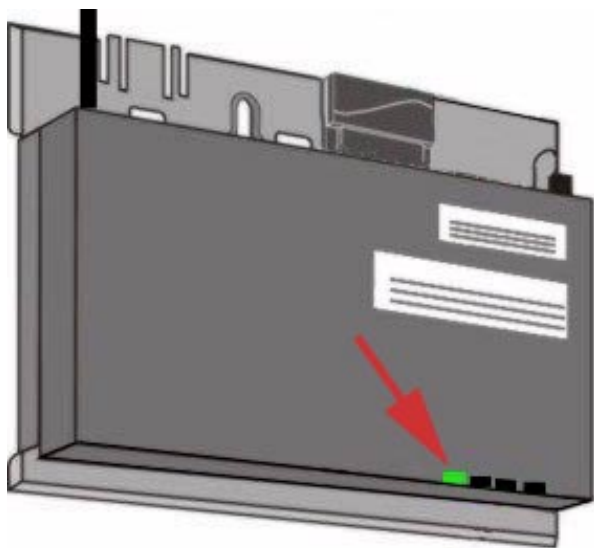


Figure 2-8 Power LED turns green when the unit is operational

9. Determine the best location for your device.

Installation & Basic Configuration

⇒ NOTE

Proxim recommends that you perform a Site Survey prior to determine the installation location for your AP-2500. For information about how to conduct a Site Survey, contact your local reseller.

10. Once you have chosen a final location for your unit, mount the wall bracket and the processor module and place the cover onto the unit as shown.

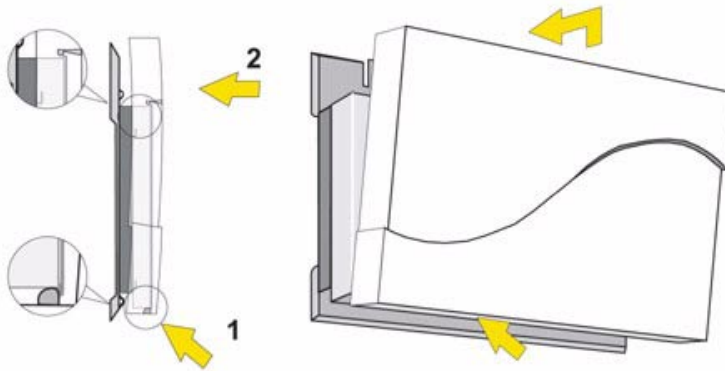


Figure 2-9 Wall mounting the AP

Installing a Card in Slot B

The AP-2500 ships with a metal faceplate that covers Slot B, shown below.



Figure 2-10 Metal Faceplate

This faceplate is required to satisfy safety regulations for installing the AP in plenum space (see [Installing the AP-2500 in a Plenum](#)). You must remove this faceplate to install a second radio card.

Follow these steps to remove the faceplate:

1. Disconnect the power and Ethernet cables from the AP (if necessary).
2. Locate a thin flathead screwdriver.
3. Place the screwdriver under the tab of the faceplate.
4. Apply torque upwards to snap the plate off the AP.

5 GHz Kit Installation

⇒ NOTE

You can install one 5 GHz (IEEE 802.11a) adapter in each AP, or you can use one 2.4 GHz (802.11b) card and one 5 GHz adapter card.

1. Disconnect power to the AP by unplugging the power supply from the power source or removing the Ethernet cable from the Active Ethernet power injector.
2. Remove the unit from its mounting location - keep the mounting bracket with the AP.
3. Remove the outer plastic cover.

Installation & Basic Configuration

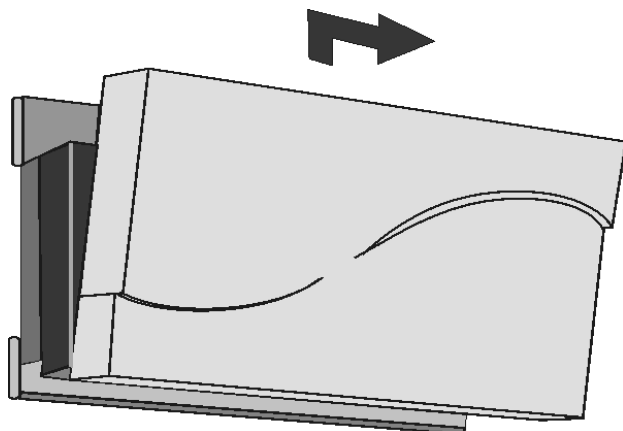


Figure 2-11 Remove the AP cover

4. Remove the power and Ethernet cables from the unit.
5. Position the antenna adapter, card inward, facing the top of the unit (see diagram) and insert the 5 GHz card into the available card slot.

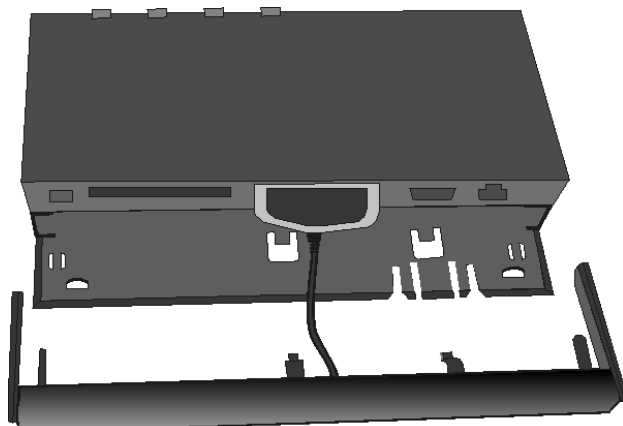


Figure 2-12 Insert card

6. Angle the antenna adapter slightly upwards, pinch the end tabs inwards and carefully slide the antenna adapter onto the mounting bracket.
7. Gently push forward while rotating the antenna downwards and clip the adapter into the small cutouts on the face of the mounting bracket.

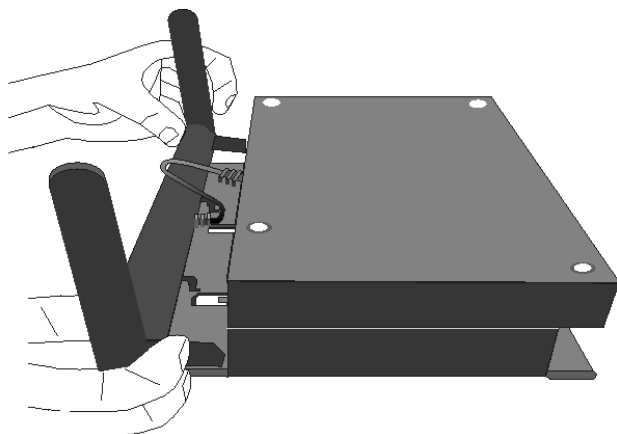


Figure 2-13 Insert antenna

Installation & Basic Configuration

8. Position the antenna for best reception:
 - at a 90° angle for flat surface mounts
 - at a 180° angle for wall mounts
9. Re-attach the power and Ethernet cabling.
10. Re-install the cover and mount the AP back in place.
11. Re-connect the power supply to the power source or the Ethernet cable to the AE power injector.

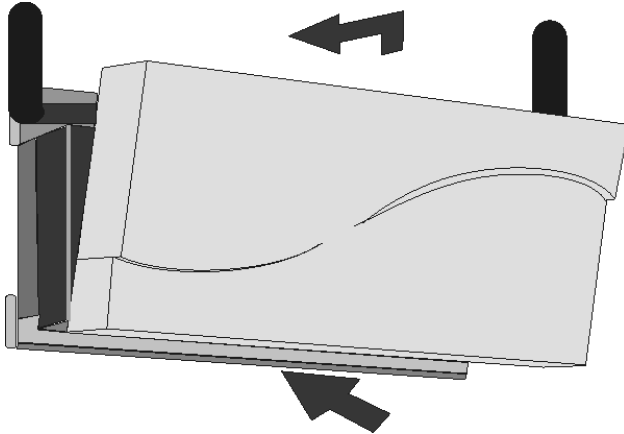


Figure 2-14 Replace cover

Installing the AP-2500 in a Plenum

In an office building, plenum is the space between the structural ceiling and the tile ceiling that is provided to help air circulate. Many companies also use the plenum to house communication equipment and cables. However, these products and cables must comply with certain safety requirements, such as Underwriter Labs (UL) Standard 2043: "Standard for Fire Test for Heat and Visible Smoke Release for Discrete Products and Their Accessories Installed in Air-Handling Spaces."

The AP-2500 has been certified under UL Standard 2043 and can be installed in the plenum only when the following conditions apply:

- The AP's plastic cover has been removed.
- There are two 802.11b cards installed in the card slots OR there is only one 802.11b card installed and the other card slot is protected with the metal faceplate shipped with the unit from the factory.



NOTE

The AP-2500 using the 5 GHz Upgrade Kit is not certified for plenum installation.

Installation & Basic Configuration

Initialization (ScanTool)

ScanTool is a software utility that is included on the installation CD-ROM. The tool automatically detects the Access Points installed on your network, regardless of IP address, and lets you configure each unit's IP settings. In addition, you can use ScanTool to download new software to an AP that does not have a valid software image installed (see [Download a New Image Using ScanTool](#)).

⇒ NOTE

These initialization instructions describe how to configure an AP-2500 over an Ethernet connection using ScanTool and the HTTP interface. If you want to configure the unit over the serial port, see [Setting IP Address using Serial Port and Normal CLI](#) for information on how to access the CLI over a serial connection and [Using the Command Line Interface](#) for a list of supported commands.

To access the HTTP interface and configure the AP-2500, the AP must first be assigned an IP address that is valid on its Ethernet network. By default, the AP-2500 is assigned a static IP address of 10.0.0.10 with a 255.255.255.0 subnet mask.

ScanTool Instructions

Follow these steps to install ScanTool and set the Access Point's basic IP settings:

1. Locate the unit's Ethernet MAC address and write it down for future reference. The MAC address is printed on the product label. Each unit has a unique MAC address, which is assigned at the factory.
2. Confirm that the AP is connected to the same LAN subnet as the computer that you will use to configure the AP.
3. Turn on the AP, if necessary.
4. Insert the ORiNOCO CD into the CD-ROM drive of the computer that you will use to configure the AP.
 - Result: The installation program will launch automatically.
5. Follow the on-screen instructions to install the Access Point software and documentation.
 - The installation program supports the following operating systems:
 - Windows 98
 - Windows 2000
 - Windows ME
 - Windows XP
6. After the software has been installed, double-click the **ScanTool** icon on the Windows desktop to launch the program (if the program is not already running).
 - Result: ScanTool scans the subnet and displays all detected ORiNOCO Access Points. The ScanTool's **Scan List** screen appears, as shown in the following example.

⇒ NOTE

If your computer has more than one network adapter installed, you will be prompted to select the adapter that you want ScanTool to use before the **Scan List** appears. If prompted, select an adapter and click **OK**. You can change your adapter setting at any time by clicking the **Select Adapter** button on the **Scan List** screen. Note that the **ScanTool Network Adapter Selection** screen will not appear if your computer only has one network adapter installed.

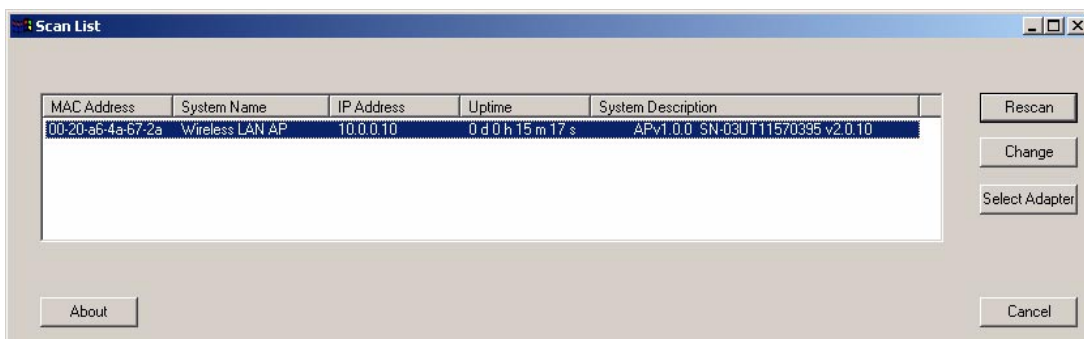


Figure 2-15 Scan List

Installation & Basic Configuration

7. Locate the MAC address of the AP you want to initialize within the Scan List.



NOTE

If your Access Point does not show up in the Scan List, click the **Rescan** button to update the display. If the unit still does not appear in the list, see [Troubleshooting](#) for suggestions. Note that after rebooting an Access Point, it may take up to five minutes for the unit to appear in the Scan List.

8. Highlight the AP's entry and click the **Change** button.
 - Result: the **Change** screen appears.

Figure 2-16 Scan Tool Change Screen

9. Configure the **IP Address Type** to **Static** or **Dynamic**.
 - The AP will become a Dynamic Host Configuration Protocol (DHCP) client when **IP Address Type** is set to **Dynamic**. Note that it requests an IP address only during boot-up (so it will not obtain an IP address if you connect it to the Ethernet after turning it on).
 - Proxim recommends that you assign the AP-2500 a static public IP address (that is, an address that is routable on the Internet). Some of the Public Space features will not work properly if the AP's IP address changes at a later date.
10. If you set IP Address Type to Static, follow these additional steps:
 - Enter a static **IP Address** for the AP-2500 in the field provided. This should be a routable public IP address. Contact your network administrator if you need assistance selecting an IP address for the unit.
 - Enter your network's **Subnet Mask** in the field provided.
 - Enter your network's **Gateway IP Address** in the field provided.
11. Enter the SNMP Read/Write password in the **Read/Write Password** field (for new units, the default SNMP Read/Write password is "public").



NOTE

The TFTP Server IP Address and Image File Name fields are only available if ScanTool detects that the AP does not have a valid software image installed. See [Download a New Image Using ScanTool](#).

1. Click **OK** to save your changes.
 - Result: The Access Point will reboot automatically and any changes you made will take effect.
2. When prompted, click **OK** a second time to return to the **Scan List** screen.
3. Click **Cancel** to close the ScanTool.

Installation & Basic Configuration

Basic Configuration

Once you have a valid IP Address assigned to your AP-2500 and you can communicate with it over an Ethernet network, use your web browser to configure the AP-2500. This section describes how to perform some basic functions and configure some of the AP's basic settings to get you started.

- [Logging into the Web Interface](#)
- [Set System Name, Location and Contact Information](#)
- [Set the Access Point's IP Address](#)
- [Configure Network Names for the Wireless Interfaces](#)
- [Configure the Ethernet Interface](#)
- [Set WEP Encryption for each Wireless Interface](#)
- [Set and Change Passwords](#)
- [Configure the Date and Time](#)
- [Reboot the AP](#)



NOTE

After configuring the basic settings, reboot the Access Point so your changes will take effect.

Logging into the Web Interface

Follow these steps to access the Access Point's Web interface:

1. Open a Web browser on a network computer on the same Ethernet network as the AP.
 - The Web browser interface supports the following Web browser
 - Microsoft Internet Explorer 5.5 or later
 - Netscape 6 or later



NOTE

For security reasons, the AP-2500 can only be configured over its Ethernet port. You cannot configure the AP using a wireless client.

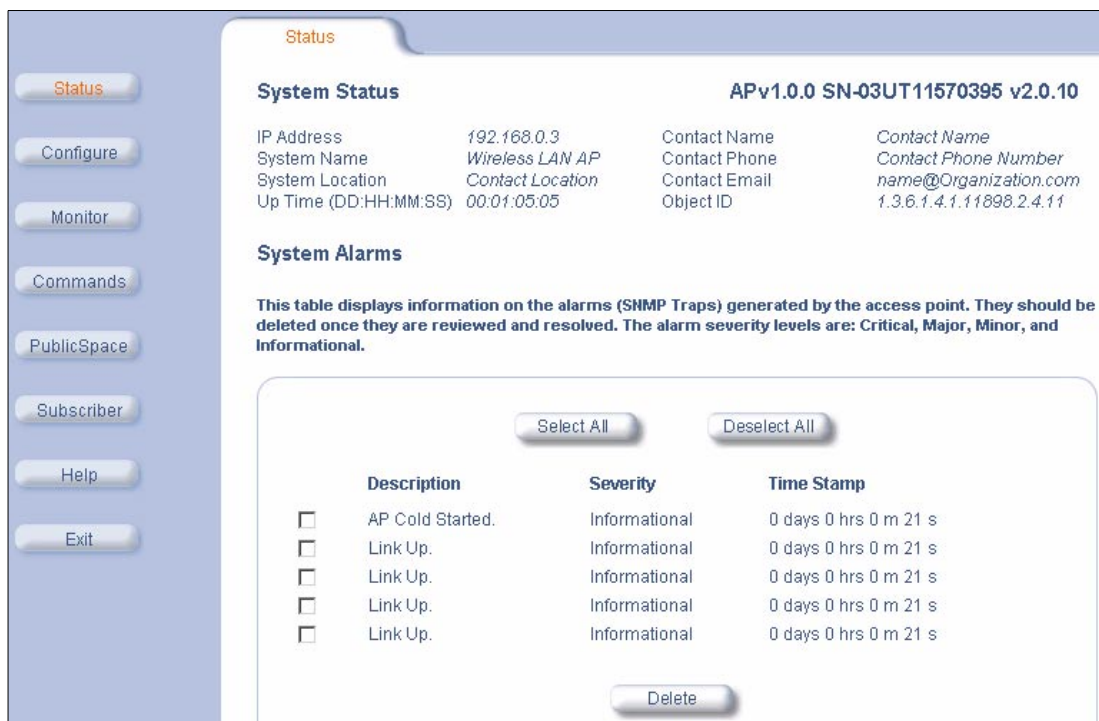
2. If necessary, disable the browser's Internet proxy settings. For Internet Explorer users, follow these steps:
 - Select **Tools > Internet Options...**
 - Click the **Connections** tab.
 - Click **LAN Settings...**
 - If necessary, remove the check mark from the **Use a proxy server** box.
 - Click **OK** twice to save your changes and return to Internet Explorer.
3. Enter the Access Point's IP address in the browser's **Address** field and press **Enter**.
 - This is either the dynamic IP address assigned by a network DHCP server or the static IP address you manually configured. See [Initialization \(ScanTool\)](#) for information on how to determine the unit's IP address and manually configure a new IP address, if necessary.
 - Result: The **Enter Network Password** screen appears.
4. Enter the HTTP password in the **Password** field. Leave the **User Name** field blank. For new units, the default HTTP password is "public".
 - Result: The **System Configuration** screen appears.

Installation & Basic Configuration



The dialog box titled "Enter Network Password" contains a key icon and the instruction "Please type your user name and password." It includes fields for "Site:" (192.168.0.3), "Realm:" (Access-Product), "User Name" (empty), and "Password" (masked with 'x'). There is a checkbox for "Save this password in your password list" and "OK" and "Cancel" buttons.

Figure 2-17 Enter Network Password



The "Status" screen displays system information and alarms. The left sidebar contains buttons for Status, Configure, Monitor, Commands, PublicSpace, Subscriber, Help, and Exit. The main content area shows "System Status" with fields for IP Address (192.168.0.3), System Name (Wireless LAN AP), System Location (Contact Location), Up Time (00:01:05:05), Contact Name, Contact Phone, Contact Email, and Object ID. Below this is the "System Alarms" section, which includes a table of alarms and a "Delete" button.

Description	Severity	Time Stamp
<input type="checkbox"/> AP Cold Started.	Informational	0 days 0 hrs 0 m 21 s
<input type="checkbox"/> Link Up.	Informational	0 days 0 hrs 0 m 21 s
<input type="checkbox"/> Link Up.	Informational	0 days 0 hrs 0 m 21 s
<input type="checkbox"/> Link Up.	Informational	0 days 0 hrs 0 m 21 s
<input type="checkbox"/> Link Up.	Informational	0 days 0 hrs 0 m 21 s

Figure 2-18 Web Interface's System Status Screen

Installation & Basic Configuration

Set System Name, Location and Contact Information

The screenshot shows the 'System' configuration tab in the Proxim web interface. The left sidebar contains buttons for Status, Configure (highlighted), Monitor, Commands, PublicSpace, Subscriber, Help, and Exit. The main content area has tabs for Filtering, Alarms, Bridge, Security, Network, Interfaces, and Management. The 'System' tab is active, displaying a form with the following fields and values:

Field	Value
Name	Wireless LAN AP
Location	Contact Location
Contact Name	Contact Name
Contact Email	name@Organization.com
Contact Phone	Contact Phone Number
Object ID	1.3.6.1.4.1.11898.2.4.11
Ethernet MAC Address	00:20:A6:4A:67:2A
Descriptor	APv1.0.0 SN-03UT11570395 v2.0.10
Up Time (DD:HH:MM:SS)	00:01:16:10

At the bottom of the form are 'OK' and 'Cancel' buttons. A note at the top of the form states: 'This tab allows for configuration of system unique parameters and contact information. Note: Changes to these parameters require access point reboot in order to take effect.'

Figure 2-19 System Configuration

1. Click **Configure > System**.
2. Enter a name for the AP, its location within your network or its physical location (such as "Front Lobby" or Engineering), and the name, phone number, and e-mail address of the person responsible for this device.
3. Click **OK**.

Set the Access Point's IP Address

You should have already assigned the Access Point an IP address using ScanTool (see [Initialization \(ScanTool\)](#)) or the CLI (see [Using the Command Line Interface](#)). However, follow these steps if you want to change the Access Point's IP address:

1. Click **Configure > Network**.
2. Set the **IP Address Assignment Type (Dynamic or Static)**.



NOTE

For best results, Proxim recommends that you assign the AP-2500 a static public IP address that is routable on the Internet. If you use a dynamic IP address, some of the Public Space features may not work properly if the IP address changes at a later date.

3. If you set the IP Address Assignment Type to Static, enter the following information in the fields provided:
 - **Network IP Address**
 - **Network Subnet Mask**
 - **Default Gateway IP Address**



NOTE

The AP's Subnet Mask needs to match the Subnet Mask of your network.

4. Click **OK** when finished. The AP-2500 unit will need to be rebooted for the changes to take effect.

The screenshot displays the Proxim Wireless Networks configuration web interface. On the left is a sidebar with buttons: Status, Configure (highlighted), Monitor, Commands, PublicSpace, Subscriber, Help, and Exit. The main area has a top navigation bar with tabs: Filtering, Alarms, Bridge, Security, System, Network (highlighted), Interfaces, and Management. Below this is a sub-navigation bar with tabs: IP Configuration (highlighted), DHCP Server, DNS Server, and VLAN. The IP Configuration tab contains the following text: "This tab is used to configure the internet (TCP/IP) settings for the access point. These settings can be either entered manually (static IP address, subnet mask, and gateway IP address) or obtained automatically (dynamic)." and a note: "Note: Changes to these parameters require access point reboot in order to take effect." Below the text are four input fields: IP Address Assignment Type (set to Static), Network IP Address (135.156.20.148), Network Subnet Mask (255.255.255.0), and Gateway IP Address (135.156.20.1). At the bottom are OK and Cancel buttons.

Figure 2-20 Network IP Configuration

Configure Network Names for the Wireless Interfaces

During boot-up, the AP automatically detects the number and type of radio cards installed and updates the wireless configuration parameters accordingly. Many of the wireless settings can be left at their default value.

However, you may want to change the Network Name for each wireless interface. By default, Slot A's Network Name is "My Wireless Network A" and Slot B's Network Name is "My Wireless Network B".

1. Click **Configure** > **Interfaces** > **Wireless-A** (slot A) or **Wireless-B** (slot B) to view the Wireless configuration options for the installed card.
2. Enter a Network Name (between 1 and 31 characters) in the **Network Name (SSID)** field.
 - The Network Name is also known as the Service Set ID (SSID).
3. Click **OK**.

A wireless client must have either the same Network Name as the AP or a Network Name of "any" to communicate with an AP.

The AP includes a feature called **Closed System** for 802.11b cards that prevents clients with a Network Name of "any" from communicating with the AP. If you want to enable Closed System, keep in mind that you will need to inform subscribers of the Network Name and they will need to change this setting on their computer before gaining access to the network.

See [Wireless \(802.11a\)](#) for more information on the AP's 802.11a wireless features and [Wireless \(802.11b\)](#) for more information on the AP's 802.11b wireless features.

Configure the Ethernet Interface

1. Click **Configure > Interfaces > Ethernet**.
2. Set the Speed and Transmission Mode for the AP's Ethernet interface.
 - This is the speed and duplex at which the AP communicates with your Ethernet network. By default, the AP automatically detects the settings of the hub or switch to which it is connected. If you are having problems communicating with the AP over the Ethernet, manually set the mode to match your hub or switch's settings. Options include:
 - 10 Mbits/sec and half-duplex
 - 10 Mbits/sec and full-duplex
 - 10 Mbits/sec and auto-duplex
 - 100 Mbits/sec and half-duplex
 - 100 Mbits/sec and full-duplex
 - Auto-speed and auto-duplex (the default setting)
3. Click **OK**.

Set WEP Encryption for each Wireless Interface

The IEEE 802.11 standards specify an optional encryption feature, known as Wired Equivalent Privacy or WEP, that is designed to provide a wireless LAN with a security level equal to what is found on a wired Ethernet network. WEP encrypts the data portion of each packet exchanged on an 802.11 network using an Encryption Key (also known as a WEP Key).

When Encryption is enabled, two 802.11 devices must have the same Encryption Keys and both devices must be configured to use Encryption in order to communicate. If one device is configured to use Encryption but a second device is not, then the two devices will not communicate, even if both devices have the same Encryption Keys.

- The AP-2500 supports 64-bit and 128-bit encryption (for both 802.11a and 802.11b), depending on the type of cards inserted into the AP's slots.
 - For 64-bit encryption, an encryption key is 10 hexadecimal characters (0-9 and A-F) or 5 ASCII characters (see [ASCII Character Chart](#)).
 - For 128-bit encryption, an encryption key is 26 hexadecimal characters or 13 ASCII characters. Note that some 802.11b cards do not support 128-bit encryption.



NOTE

64-bit encryption is sometimes referred to as 40-bit encryption; 128-bit encryption is sometimes referred to as 104-bit encryption.

Keep in mind that if you enable WEP encryption on the wireless interfaces, you will need to inform your subscribers of these settings and they will need to reconfigure their wireless cards with these settings before gaining access to the network (and before they are prompted to logon to the hotspot).

Follow these steps to configure WEP:

1. Click **Configure > Security > Encryption**.
2. Place a check mark in the **Enable Encryption (WEP)** boxes as necessary.
 - If you only have one wireless card installed, only one box will appear; two boxes appear if you have two cards installed.
 - If two cards are installed, you can enable encryption for either or both of the wireless slots (Slot A and/or Slot B).
3. Enter one to four Encryption Keys in the fields provided. Keep in mind the following:
 - If entering more than one Key, use the same number of characters for each Key. All Keys need to be the same Key Size (64 or 128-bit). The card must support the Key Size that you specify (some 802.11b cards do not support 128-bit encryption).
 - You can enter the Encryption Keys in either hexadecimal or ASCII format.
 - You need to configure your wireless clients to use the same Keys in order for the clients and the AP to communicate. Subscribers that do not have the same encryption settings will be unable to login at the hotspot.
4. Set **Deny Non-Encrypted Data** to **Enable** if you want to prevent clients that do not have WEP enabled or the proper keys configured from communicating with the network. Enabled is the recommended settings.

Installation & Basic Configuration

5. Select the Key that the Access Point will use to encrypt outgoing data from the **Encrypt Data Transmissions Using** drop-down menu. By default, this parameter is set to Key 1.
6. Repeat these steps for the second slot (if applicable).
7. Click **OK**.
8. Reboot the AP for these changes to take effect.

The screenshot shows the 'Security' tab in the configuration interface, specifically the 'Encryption' sub-tab. The interface includes a left sidebar with buttons for Status, Configure, Monitor, Commands, PublicSpace, Subscriber, Help, and Exit. The main content area has tabs for Filtering, Alarms, Bridge, and Security. Under the Security tab, there are sub-tabs for MAC Access, RADIUS, Encryption, and VPN. The Encryption sub-tab is active and contains the following text:

This tab is used to configure encryption (WEP) in the access point. This is used to provide data security for wireless communication between the access point and wireless clients. Encryption settings can be configured for both wireless interfaces.

Note: The access point supports both 40 and 104 bit keys depending on the wireless PC card in the device. If 5 alphanumeric characters are entered for an encryption key, then the key length is 40 bits. If 13 alphanumeric characters are entered for an encryption key, then the key length is 104 bits.

Warning: Connectivity requires that encryption keys on the access point and the wireless clients be identical.

Note: Changes to these parameters require access point reboot in order to take effect.

Enable Encryption (WEP) for Slot A ☒
 Enable Encryption (WEP) for Slot B ☒

Wireless Interface	Slot A	Slot B
Encryption Key 1	*****	*****
Encryption Key 2	*****	*****
Encryption Key 3	*****	*****
Encryption Key 4	*****	*****
Deny Non-Encrypted Data	Enable	Enable
Encrypt Data Transmissions Using	Key 1	Key 1

At the bottom of the form are 'OK' and 'Cancel' buttons.

Figure 2-21 WEP Encryption

Set and Change Passwords

1. Click **Configure > Management > Passwords**.
2. Set the **SNMP Read Password**. Enter a password in both the **Password** field and the **Confirm** field.
 - An SNMP management program must be configured with this same password (also known as a community string) to gain read access to the AP. The default password is "public".
3. Set the **SNMP Read/Write Password**. Enter a password in both the **Password** field and the **Confirm** field.
 - An SNMP management program must be configured with this same password (also known as a community string) to gain read and write access to the AP. The default password is "public".
4. Set the **Telnet (CLI) Password**. Enter a password in both the **Password** field and the **Confirm** field.
 - This is the password for the CLI interface (whether you access it via Telnet or the AP's serial port). The default password is "public".
5. Set the **HTTP (Web) Password**. Enter a password in both the **Password** field and the **Confirm** field.
 - This is the password for the HTTP Web browser interface. The default password is "public".
6. Click **OK**.

Installation & Basic Configuration

NOTE

For security purposes Proxim recommends that you change ALL PASSWORDS from the default “public” immediately to restrict access to authorized personnel. If you lose or forget your password settings, you can always perform the [Reset to Factory Default Procedure](#).

Configure the Date and Time

The AP boots up using January 1, 1970 as the date and 00:00:00 as the time. The AP does not necessarily need the correct date and time but you may want the AP to report the correct date and time if you intend to enable the [Logging](#) (Syslog) or [Credit Card Mirroring](#) functionality. Note that the AP's [System Status](#) alarms are reported in terms of the AP's **Up Time** and not in terms of standard date and time.

You can either manually set the date and time or configure the AP to contact a time server on the Internet during boot-up to retrieve the correct date and time.

Configuring the Date/Time Using NTP

If you want the AP to use the Network Time Protocol (NTP) to retrieve the time over the Internet, keep in mind the following:

- The AP will only contact a time server during boot-up. Therefore, you need to reboot the AP after configuring this.
- The AP must have a connection to the Internet to retrieve the date and time.
- See <http://www.ntp.org/> to identify the IP addresses for public time servers in your area.

Follow these steps to configure the AP to use NTP:

1. Click **Configure > Management > NTP**.
2. Place a check mark in the **Enable NTP** box.
3. Enter the IP address for a public time server in the **Primary Time Server** box.
4. Enter the IP address of a second public time server in the **Secondary Time Server** box.
 - This field is optional. The AP will attempt to contact the secondary server if the first is unavailable.
5. Select your time zone from the **Time Zone** drop-down menu.
6. Select the appropriate **Day Light Saving** option from the drop-down menu.
 - For example, if your location is currently using Day Light Saving time (from April to October in most of the U.S.), set this parameter to **+1** to adjust for day light savings time.
 - If in doubt, leave this field blank. If you notice that the time is off by one or two hours following a reboot, check the time zone or adjust the Day Light Saving setting accordingly.
7. Click **OK**.
8. Reboot the AP for this change to take effect.

Configuring the Date/Time Manually

1. Click **Configure > Management > NTP**.
2. Scroll down to the **Set Date and Time** heading.
3. Enter the **Year** (yyyy).
4. Enter the **Month** (1-12).
5. Enter the **Day** (1-31).
6. Enter the **Hour** (0-23).
7. Enter the **Minute** (0-59).
8. Enter the **Second** (0-59).
9. Click **OK**.

NOTE

These changes take effect immediately. However, the date and time will be reset to January 1, 1970, 00:00:00 the next time you reboot (unless you have NTP enabled and the AP successfully contacts a time server).

Installation & Basic Configuration

Reboot the AP

Most of the AP's configuration settings take effect immediately; they do not require a reboot. However, some parameters do require a reboot before they take effect. Therefore, reboot the AP after configuring the basic settings to ensure that all of your changes take effect.

1. Click **Commands > Reboot**.
2. Click **OK** to reboot the unit immediately.

NOTE

Wait for the unit's Power LED to turn green before attempting to browse any other page. Also, if you changed the unit's IP address, you will need to enter the new address in your browser.

Download the Latest Software

Proxim periodically releases updated software for the AP on its Web site at <http://www.proxim.com/>. Proxim recommends that you check the Web site for the latest updates after you have installed and initialized the unit.

Four types of files can be downloaded to the AP from a TFTP server:

- Img (AP software image)
- Config (configuration file)
- bspBI (BSP/Bootloader firmware file)
- Generic (everything else; primarily this refers to files related to the Public Access features)

Setup your TFTP Server

A Trivial File Transfer Protocol (TFTP) server allows you to transfer files across a network. You can upload files from the AP for backup or copying, and you can download the files for configuration and AP Image upgrades. The Solarwinds TFTP server software is located on the installation CD-ROM. You can also download the latest TFTP software from Solarwind's Web site at <http://www.solarwinds.net/>.

If a TFTP server is not configured and running, you will not be able to download and upload images and configuration files to/from the AP. Remember that the TFTP server does not have to be local as long as you have a valid TFTP server IP address. Also, note that a TFTP server does not have to be running for the AP to perform tasks that do not involve file transfers.

After the TFTP server is installed:

- Check to see that the TFTP program is configured to point to the directory containing the AP Image.
- Make sure you have the proper TFTP server IP address, the proper AP Image file name, and that the TFTP server is operational.
- **Make sure the TFTP server is configured to both Transmit and Receive files, with no automatic shutdown or time-out.**

Download Updates from your TFTP Server using the Web Interface

1. Download the latest software at <http://www.proxim.com/>.
2. Copy the latest software updates to your TFTP server.
3. In the Web Interface, click **Commands > Download**.
4. Enter the IP address of your TFTP server in the field provided.
5. Enter the **File Name** (including the file extension). Enter the full directory path and file name. If the file is located in the default TFTP directory, you need enter only the file name.
6. Select the **File Type** from the drop-down menu (use *Img* for software updates).
7. Select **Download & Reboot** from the **File Operation** drop-down menu.
8. Click **OK**.
9. The Access Point will reboot automatically when the download is complete.

Installation & Basic Configuration

Download Updates from your TFTP Server using the CLI Interface

1. Download the latest software at <http://www.proxim.com/>.
2. Copy the latest software updates to your TFTP server.
3. Open the CLI interface via Telnet or a serial connection. (See [Using the Command Line Interface](#) for more information.)
4. Enter the CLI password when prompted.
5. Type **set tftpfilename <file name>** (include the file extension) and press **Enter**.
6. Type **set tftpfiletype img** and press **Enter**.
7. Type **set tftpipaddr <IP address of your TFTP server>** and press **Enter**.
8. Type **show tftp** and confirm that the file name, file type, and IP address are correct.
9. Type **download *** and press **Enter**.
 - Result: The download will begin. Be patient while the image is downloaded to the Access Point.
10. When the download is complete, type **reboot 0** and press **Enter**.

Back-up the AP's Configuration Files

After you have configured the AP, you may want to back-up its configuration files for safekeeping. Once you have uploaded the files, you can download them to the AP at a later date and return its configuration to the settings specified in the back-up files.

There are two configuration files for the AP-2500: one file contains the Network settings (that correspond to the parameters described in the ORINOCO MIB) and the second file contains the Public Space settings (that correspond to the parameters described in the Nomadix MIB). See [SNMP Management](#) for more information on the MIB files.

The file that contains the Network settings uses the **Config** file type and can use any file name. Proxim recommends that you use **config.sys** as the file name (this is the name used in the instructions below).

The file that contains the Public Space settings uses the **Generic** file type and the file name is **current.txt** (you must use this file name for the Public Space settings).

Uploading Configuration Files

Follow these steps to upload the AP's configuration files to a TFTP server:

1. Login to the AP's Web browser interface.
 2. Click **Commands > Upload**.
 3. Enter the IP address of the computer running the TFTP server application in the **Server IP Address** field.
 4. Enter **config.sys** in the **File Name** field.
 5. Set the **File Type** to **Config**.
 6. Click **OK**.
 - Result: The TFTP operation begins. A new **TFTP Operation Status** window opens.
 7. Click **Close** after the TFTP operation is complete.
 8. Enter **current.txt** in the **File Name** field.
 9. Set the **File Type** to **Generic**.
 10. Click **OK**.
 - Result: The TFTP operation begins. A new **TFTP Operation Status** window opens.
 11. Click **Close** after the TFTP operation is complete.
- Copies of the AP's configuration files (**config.sys** and **current.txt**) should now be in your TFTP server's root directory.

Installation & Basic Configuration

Downloading Configuration Files

Follow these steps to download configuration files to the AP:

1. Copy *config.sys* and *current.txt* to your TFTP server's root directory (if necessary).
2. Login to the AP's Web browser interface.
3. Click **Commands > Download**.
4. Enter the IP address of the computer running the TFTP server application in the **Server IP Address** field.
5. Enter **current.txt** in the File Name field.
6. Set the **File Type** to **Generic**.
7. Set **File Operation** to **Download**.
8. Click **OK**.
 - Result: The TFTP operation begins. A new **TFTP Operation Status** window opens.
9. Click **Close** after the TFTP operation is complete.
10. Enter **config.sys** in the **File Name** field.
11. Set the **File Type** to **Config**.
12. Set **File Operation** to **Download & Reboot**.
13. Click **OK**.
 - Result: The TFTP operation begins. A new **TFTP Operation Status** window opens.
14. Click **Close** after the TFTP operation is complete.

The AP should reboot automatically after uploading the **config.sys** file. Following the reboot, the AP will use the settings contained in the **config.sys** and **current.txt** files you downloaded to the unit.

Public Space and Advanced Configuration

Once you've configured the basic settings and have become comfortable with using the AP's Web browser interface, you can configure the AP's Public Space feature and advanced networking features.

- See [AP-2500 Authentication Methods](#) for information on the Public Space Authentication techniques supported by the AP-2500.
- See [Network Parameters](#) for information on the AP's networking features. This section provides information for each of the networking features that you can configure using the Web browser interface. These are the network settings that are available with most traditional access points (although some features, such as [DHCP Server](#), play an important role in hotspot operation).
- See [Public Space Parameters](#) for information on the AP's Public Space features. This section provides information for each of the Public Space features that you can configure using the Web browser interface. The Public Space features are what make the AP-2500 unique among access points.

3

AP-2500 Authentication Methods

The AP-2500 is a versatile Access Point for hotspot locations that supports multiple authentication methods. The unit includes all of the features necessary for a user to set up a hotspot quickly and easily without requiring servers or advanced Web design skills. The AP-2500 also integrates into existing billing or authentication solutions (for example, if you already have a RADIUS server on your network that performs authentication and accounting tasks).

Authentication Overview

Providing Internet access to customers represents a new revenue generator or value-add service for public locations such as coffee shops, bookstores, and hotels. In a traditional Access Point model, the network authenticates users for security reasons (to prevent unauthorized users from accessing the system). But a public gateway Access Point (such as the AP-2500) takes this a step further and provides authentication services for paying subscribers. When a user enters a coffee shop with an 802.11-compatible laptop and launches his Web browser, he is immediately directed to a subscriber login page. If currently a customer, the subscriber enters his user name and password to gain access. If not a current subscriber, the user can select an access plan and pay for connectivity by credit card before gaining access to the Internet.

The AP-2500 supports multiple authentication techniques to suit a range of users. If you're new to the hotspot market, you can enable the AP to use its Internal Web Server and login page. This method is easy to setup but provides less customization options than the more complicated techniques that involve other servers on your network, such as a RADIUS server or an External Web Server.

The AP-2500 supports the following authentication methods:

- **No Authentication**
The AP's Authentication, Authorization, and Accounting (AAA) services are disabled. Subscribers can access the Internet through the AP-2500 without being authenticated first. This is the AP's default setting.
- [Internal Authentication](#)
The AP provides all authentication services using its Internal Web Server (IWS), including an internal login page. It also maintains a list of customers in its Authorized Subscribers Table. You can configure the AP to support credit card billing for new subscribers in this configuration. More advanced users can also create a portal page, which appears to customers before the login screen. The portal page resides on an external Web server on the hotspot's network and provides additional customization and access to free content (also known as a "walled garden").
- [Internal Authentication with RADIUS](#)
In this configuration, the AP still provides all of the services described above, but it also communicates with a RADIUS server on the network to determine if a user is valid. The RADIUS server maintains a list of subscribers and their attributes (such as the maximum bandwidth allowed for a specific customer) that it communicates back to the AP-2500. The RADIUS server can also perform accounting functions to record a user's login activity to facilitate billing.
- [External Authentication](#)
In this configuration, the authentication procedure is handled outside of the AP by an External Web Server (EWS). The AP is notified by an external server when a user has been authenticated using XML (Extensible Markup Language) commands. This configuration is intended for advanced users who have some background in Web design.

The following sections provide detailed information and step-by-step configuration instructions for each of the authentication methods described above (except for the "no authentication" option).

AP-2500 Authentication Methods

Internal Authentication

In this configuration, the AP-2500 provides all authentication services to subscribers using its Internal Web Server (IWS). This is the easiest configuration to design and implement but it offers limited functionality.

The following diagram illustrates a network topology using the AP's internal authentication services:

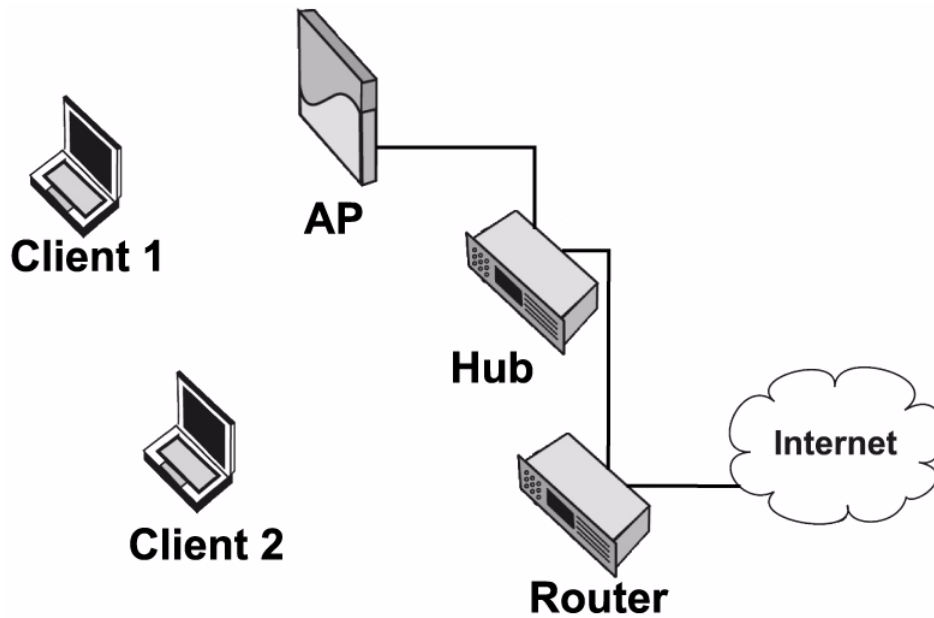


Figure 3-1 Network Using Internal Web Server



NOTE

You can connect the AP-2500 directly to a router, DSL modem, or another Internet device once it has been properly configured, if necessary. For example, you may want to connect the AP directly to your Internet device if your ISP only provides you with one public IP address. However, note that the AP can only be managed over its Ethernet or serial port. Therefore, if you choose to connect it directly to your Internet device, you may not be able to manage the AP without first disconnecting it from the Internet device (which will force all subscribers to lose their Internet connection).

This configuration offers three billing models:

1. **Rent wireless cards to customers for cash:** The hotspot operator maintains an inventory of wireless cards whose Media Access Control (MAC) addresses are listed in the AP-2500's Authorized Subscribers Table. Only these cards can gain access to the network. Customers pay cash to rent cards for a specified period of time from the hotspot operator. Note that this configuration does not require an account with a credit card billing service but a user may need to run an installation program to install the wireless card you provide.
2. **Manually enter customers into Authorized Subscribers Table for cash:** Subscribers pay in cash at the counter for a limited amount of access time. The hotspot operator then manually adds the user to the Authorized Subscribers Table, assigning a User Name, Password, bandwidth restrictions, and access time. The subscriber supplies his own Wi-Fi card in this configuration.
3. **Customers purchase access time via credit card:** Subscribers use their own wireless cards to communicate with the AP-2500. When prompted, the subscriber selects a billing plan and pays for access via a credit card. This configuration requires an account with a credit card billing service.

In all three cases, subscribers have Internet access for a limited period of time. The time period begins as soon as the subscriber is entered into the **Authorized Subscribers Table** (either manually or following a successful credit card purchase). Any unused time is lost. For example, if a subscriber buys two hours of access but leaves the hotspot after an hour, the subscriber loses the second hour (there is no carry over to a later date).

AP-2500 Authentication Methods

NOTE

If you want to provide the user with the ability to log in or out of the connection, you need to use a RADIUS server. See [Internal Authentication with RADIUS](#) for details.

End User Experience

The following procedure details the experience of the typical customer if you configure the AP-2500 to use internal authentication:

1. Customer enters the hotspot and turns on his laptop that has a wireless card installed.
 - If the customer is renting a card or you are manually entering customers in the [Authorized Subscribers](#) Table, the customer will need to sign up for service at the counter before turning on the laptop.
2. The wireless card associates with the AP. If the card is configured as a DHCP client, the AP automatically assigns the card a dynamic IP address.
 - The AP adds the client to its [Current Subscribers Table](#) with State set to "Pending".
3. The customer launches his Web browser. Typically, the Web browser will attempt to access its default home page.
4. The customer is automatically redirected to the AP's internal login page or to a [Portal Page](#).
 - The AP redirects the customer when it receives an HTTP request from the customer's browser.
 - If the browser's default home page is loaded in the browser's cache, the customer may not be redirected to the login screen. But the customer will be redirected the first time he tries to access a new Web site.
 - The customer must try to access a valid Web site to call up the login screen. Entering an unreachable URL or invalid Web address will not bring up the login screen.
 - Customers who try to access e-mail first will not have a connection. Customers need to login via a Web browser first.
5. If an existing customer (that is, the customer is already in the AP's [Authorized Subscribers](#) Table), the customer enters his user name and password (if enabled). If authenticating based on MAC address, the customer only clicks a **Login** button. If a new subscriber using a credit card:
 - The customer clicks the **New User** button.
 - The customer selects one of the available billing plans and the amount of time he wants to purchase.
 - The customer confirms his purchase and then enters his credit card information to pay for the access time.
 - The AP adds the customer to the [Authorized Subscribers](#) Table after a successful credit card transaction.
6. The AP authenticates the user based on the User Name/Password or MAC address. The AP updates the client's State to "Valid" in the [Current Subscribers Table](#).
7. Following successful authentication, the customer is automatically redirected to the URL of your choice (if **Home Page Redirection** is enabled) or to the page that the customer originally requested (which started the login process).
8. If the Information and Control Console is enabled, a Java window will appear on the subscriber's screen that contains information about the connection (such as time remaining) and advertising banners.

Configuration Instructions

Follow these steps to configure an AP-2500 to perform internal authentication:

1. Configure the AP-2500's basic settings. This includes the AP's IP address, System parameters, and management passwords. See [Basic Configuration](#) for details.
2. If not already open, access the AP's Web browser interface. (See [Logging into the Web Interface](#) for instructions.)
3. Click **Configure > Network > DHCP Server** to configure the AP's [DHCP Server](#) settings. The default setting should be suitable for most networks.
 - By default, the AP is configured to provide IP addresses to subscribers in the range of 10.0.0.12 to 10.0.0.36 with a 255.255.255.0 subnet mask. This is a private IP range. In most configurations, you should have assigned the AP a public IP address (that is, an address valid on the Internet). Using the default settings, the AP performs Network Address Translation (NAT) to provide Internet access to its clients. See [Dynamic Address Translation \(DAT\)](#) for more information on NAT.
 - You should change the default address range if it conflicts with the settings of another DHCP server on your network. Also, before modifying the AP's address pool, confirm that there is not another DHCP server on the network already serving addresses from this particular address range.

AP-2500 Authentication Methods

- You can disable the AP's DHCP server if there is another DHCP server that you want to use instead. See [Disabling the AP's DHCP Server](#) for details.
- 4. Configure **IP Upsell**, if desired. See [IP Upsell](#) for details.
 - In general, it costs more to obtain public IP addresses from your ISP due to limited availability. If you have a pool of public IP addresses that you can distribute, you can offer standard customers less expensive private IP addresses and premium customers public IP addresses. This concept is known as "IP Upsell".
 - Some applications require a public IP address to function properly over the Internet (such as certain VPN applications, on-line gaming, and Web hosting). Customers who require a public IP address may be willing to pay a premium for this service.
 - The subscriber's wireless card must be configured to obtain an IP address from a DHCP server to use the IP Upsell feature (that is, this feature doesn't work if the subscriber's computer is assigned a static IP address).
- 5. Click **OK** to save your changes to the DHCP Server settings.
- 6. Click the **DNS Server** tab to configure Domain Name Service (DNS) settings. This information may already be provided for you if the AP's **IP Address Type** is **Dynamic**.
 - Enter a **DNS Host Name** for the AP. The default setting is suitable for most configurations unless you have multiple APs and want to assign each one a different Host Name.
 - Enter the **DNS Domain** name. This name is provided by your ISP or network administrator.
 - Enter up to three DNS Server IP addresses in the fields provided. You must configure at least the Primary DNS Server IP address. These IP addresses should be provided by your ISP or network administrator.



NOTE

The AP must be configured with a valid DNS Server IP address to function correctly. If you are setting up a demo with this equipment, the AP must be able to communicate with a valid DNS server before it will function as expected. If you do not configure DNS, then all Internet locations must be in IP address format, including HTTP requests from subscribers.

7. Click **OK** to save your changes to the DNS Server settings.
8. Click the **Public Space** button.
9. Click the **AAA** tab.
10. Place a check mark in the **Enable AAA Services** box.
11. Set **Authorization Method** to **Internal** (this is the default setting).

The screenshot shows the 'AAA' configuration window. The 'Basic' sub-tab is selected. The text inside reads: 'This tab is used to configure the basic settings for Authentication, Authorization and Accounting (AAA) service.' Below this is a note: 'Note: If XML Interface is enabled, XML Sender IP address field must be entered.' The configuration options are: 'Enable AAA Services' (checked), 'Enable XML Interface' (unchecked), 'XML Sender IP Address' (0.0.0.0), and 'Authorization Method' (Internal selected, External unselected). 'OK' and 'Cancel' buttons are at the bottom.

Figure 3-2 AAA Configuration

AP-2500 Authentication Methods

⇒ NOTE

Advanced users can also manage the AP from a network computer using XML commands (tasks such as adding and deleting users). See [AAA Basic](#) for configuration information and [XML Interface Specification](#) for information on XML commands.

12. Click **OK** to save your changes to the AAA settings.
13. Click the **Internal** tab.
14. Configure the SSL parameters (**Enable SSL** and **Certificate DNS Name**), if desired.
 - This provides secure communication between subscribers and the AP. If you enable this feature, you will also need to upload your certificate keys to the AP. See [Secure Socket Layer \(SSL\)](#) for more information on this feature.
15. Configure the **Portal Page** parameters if you want to provide a custom “Welcome” screen for your subscribers. See [Portal Page](#) for detailed instructions and examples.
 - Place a check mark in the **Enable Portal Page** box.
 - Enter the URL for your Portal Page in the field provided.
 - The Portal Page resides on an external Web server (such as a Windows 2000 Server running Internet Information Services (IIS)) on your network.

⇒ NOTE

The **Smart Client** option is only applicable if you have enabled RADIUS. See [Smart Client](#) and [Internal Authentication with RADIUS](#) for details.

16. Configure the **Enable User Name** and **Enable New Subscribers** settings.
 - The table below describes the system response to the available User Name and New Subscribers combinations:

User Name	New Subscribers	System Response
Disabled (default)	Enabled (default)	Allows new and existing subscribers access to the network without supplying a User name and password. Authentication is based on the MAC address of the subscriber's Wi-Fi card. This setting works in conjunction with credit card services.
Enabled	Enabled	Allows new and existing subscribers access to the network after supplying a user name and password. This setting works in conjunction with credit card services.
Enabled	Disabled	Only allows existing subscribers after supplying a user name and password.
Disabled	Disabled	Only allows existing subscribers based on a card's MAC address.

Table 3-1 User Name and New Subscriber

- If you are renting cards to customers, disable User Name and New Subscribers. Only cards whose MAC addresses are entered in the Authorized Subscribers Table will have access to the Internet.
- If you are using credit card services, enable User Name and New Subscribers (if you want subscribers to create a username and password) or only enable New Subscribers (if you want subscribers to access the network based on their Wi-Fi card's MAC address).
 - The only difference between these two scenarios is that with username/password, subscribers can access the Internet from a different Wi-Fi device at a later date. For example: a subscriber purchases two days of Internet access. On the second day, the subscriber returns to the hotspot with a different Wi-Fi card. If using username/password authentication, the subscriber will be able to access the Internet using the different card with no intervention from the hotspot operator. Note that the subscriber will only be able to log in using a different Wi-Fi card if the account is not already in use (as displayed in the [Current Subscribers Table](#)). Note that a subscriber that has turned off his computer or has left the hotspot is removed from the Current Subscriber Table after 10 minutes.
- If you are manually entering user names and passwords into the Authorized Subscribers Table, enable User Name but disable New Subscribers.

AP-2500 Authentication Methods

17. If you want to charge customers for access time via credit card, configure the [Credit Card Services](#) options.
 - You need an account with a credit card service provider to use this feature.
 - The AP-2500 works with the following credit card providers by default:
 - Datacenter Luxembourg (in Europe) -- <http://www.dclux.com/>
 - ChainFusion (in Asia) -- <http://www.chainfusion.com/>
 - Authorize.net's WebLink solution (U.S.) -- <http://www.authorize.net/>
 - As of the release of this documentation, Authorize.net is discontinuing support for WebLink. Proxim is working to provide support for Authorize.net's Simple Integration Solution (SIM) method in the next AP-2500 firmware release.



NOTE

If your credit card service provider is not on the above list, you will need to provide your service provider with the [Credit Card Interface Specification](#). The credit card service provider will need to develop an interface that communicates with the AP-2500 using this specification.

- Enter the URL supplied by your credit card service provider. By default, the Authorize.net address appears in the **Credit Card Server URL** field.
 - Enter the IP address for the credit card server. By default, the Authorize.net address appears in this field (**Credit Card Server IP**). You will also need to enter this IP address in the [Passthrough Addresses](#) list.
 - Enter your **Merchant ID** (supplied by your credit card service provider) in the field provided.
18. Click **OK**.
 19. Click the **Passthrough** tab.
 20. Enter the IP Address of the external Web server that is hosting your Portal Page in the **Passthrough IP Table** (if applicable).
 21. Enter the Credit Card Server IP Address in the **Passthrough IP Table** (if applicable).
 22. Enter the DNS Names for all of the Web sites that you want to include in your "walled garden" in the **Passthrough DNS Table** (if applicable).
 - A "walled garden" is a list of Web site that your customers can access for free without logging into the AP.
 - If you want to provide free access to customers for a limited number of sites, you should use a portal page which includes links to the walled garden sites. See [Portal Page](#).
 - You can enter a single World Wide Web address (such as **www.yahoo.com**) or you can enter Domain Names (such as ***.yahoo.com**). Entering the Domain Name provides users will full access to the specified Domain's Web sites. For example, if you enter **www.yahoo.com** in the DNS Passthrough Table, customers will not be able to access sites such as **http://finance.yahoo.com** as part of the walled garden.
 23. If you plan to limit subscriber bandwidth or offer multiple access plans based on bandwidth speeds, click the **Bandwidth Mgmt** tab to notify the AP of its bandwidth settings.
 - These parameters correspond to the AP's connection to the Ethernet and the Internet. Based on these settings, the AP determines the speed of its Internet connection. The AP uses this information when making bandwidth allocations to subscribers.
 - Do not set uplink or downlink speed to 0; this will disable access to the unit over the Ethernet.
 - The upper limit for uplink or downlink speed is 100,000 Kbps (100 Mbps). This is the maximum speed at which the AP can connect to the Ethernet network. In reality, the uplink and downlink speeds will depend upon the speed of your hotspot's Internet connection (for example, T1 or DSL) and the speed of the wireless cards installed in the AP (up to 54 Mbps if using 802.11a).
 - By default, Bandwidth Management is enabled and uplink and downlink speeds are set to 1500 Kbps.
 24. If you want to redirect outgoing e-mail traffic to your Simple Mail Transfer Protocol (SMTP) server, click the **SMTP** tab and configure the SMTP Redirection settings. See [SMTP Redirection](#).
 - Most SMTP servers only transmit e-mail messages that originate from local traffic to prevent illegal use of a mail server by spammers, hackers, and other unauthorized individuals. Therefore, most of your subscribers will be unable to send email messages unless you enable SMTP Redirection.
 - When SMTP Redirection is enabled, all outgoing mail traffic is redirected to the SMTP server you specify in the **SMTP Server IP** field (this field is based on IP address and not DNS name). This will allow subscribers to send emails without changing any of the server settings in their email program. Typically, this will be your local mail server (if you have one) or your ISP's mail server.

AP-2500 Authentication Methods

- If you want all outgoing mail traffic redirected to the specified server, enable both the **Misconfigured** and **Properly Configured** options. **Misconfigured** refers to subscribers whose e-mail settings are incompatible with the AP-2500's Internet settings (in other words, these email settings may work on the subscriber's home or office network but they won't work in the hotspot); **Properly Configured** refers to subscribers whose email settings should work on the hotspot network so you do not necessarily need to redirect these messages to your own server. If you want properly configured subscribers to send mail without being redirected, enable only the **Misconfigured** option. In general, Proxim recommends that you enable both options. Also, you should never enable **Properly Configured** and disable **Misconfigured** (this combination defeats the purpose of SMTP Redirection).
- 25. If you want to redirect the user to a specified URL following successful authentication, click **HPR** and configure the Home Page Redirection options. See [Home Page Redirection \(HPR\)](#) for details.
 - If you are using a Portal Page, review [Portal Page](#) before configuring the Home Page Redirection options.
- 26. If you want a customized banner applet to appear on subscriber's browser screens, click **ICC** and configure the Information and Control Console options. See [Information and Control Console \(ICC\)](#) for details, caveats, and customization instructions.
 - The ICC is a Java applet that is pushed to your customer's Web browsers. It displays information about the user's connection (such as access time remaining) and allows your customer to dynamically change subscription plans. You can also customize the ICC's banners and buttons to promote partner Web sites.
- 27. If you want to block subscribers from accessing certain Web sites, click **URLFilter** and configure the URL Filtering options. See [URL Filtering](#) for details.
- 28. Click the **Subscriber** button.
- 29. Click the **Billing** tab and configure the **Internal Billing Options**. See [Billing Options for Subscribers](#) for details.
 - You can design up to six billing plans; the Internal Billing Options apply to all six plans. For example, if you configure **Units of Access** to Hour, all six plans must be offered on a per-hour basis.
- 30. Click the **Plan** tabs to define the billing plans that will be available to your customers. You can configure up to six plans based on price of service, bandwidth allowed, access time, and IP address type (private or public). See [Billing Options for Subscribers](#) and [IP Upsell](#) for more information.
- 31. Click the **Mirroring** tab if you want to have copies of credit card transactions sent to external servers. See [Credit Card Mirroring](#) for details.
- 32. Click the **Messages** tab to customize the messages and screens that are presented to the customer including the Login page (**Login Msgs**), general subscriber messages (**Sub Msgs**), and error messages (**Error Msgs**). See [Subscriber Messages](#) for details.
 - A default logo appears on the subscriber login page for new units. You will want to replace this logo with your own. See [Changing the Login Screen Logos](#) for detailed instructions.
- 33. If you want to manually add customers to the [Authorized Subscribers](#) Table, click the **Authorized** tab.
 - If you use Credit Card Services, subscribers are automatically added to the Authorized Subscribers Table after they have signed up and paid for an access plan.
 - If you do not use Credit Card Services or if you want to manually add a subscriber, click the **Add** button and follow these steps:
 1. Select the **DHCP Address Type** for the subscriber (public or private). This setting depends upon the [DHCP Server](#) settings you configured for the AP.
 2. If authorizing a user based on MAC address (in other words, the **PublicSpace > AAA > Internal > Enable User Name** option is disabled), enter the MAC address of the subscriber's wireless card in the field provided.
 3. You can leave the **IP Address** field blank. The AP fills in this field automatically after a subscriber logs in.
 4. If authorizing a subscriber based on user name and password (in other words, the **PublicSpace > AAA > Internal > Enable User Name** option is enabled), enter a user name and password for the subscriber.

➡ NOTE

User Name and Passwords are case-sensitive.

5. Enter the subscriber's allowed access time in the **Expiration Time** fields (in hours and/or minutes). If you leave these fields blank or set them to 0, the subscriber will never time out. If you enter hours and/or minutes, the time-out counter will begin as soon as you click **OK**. After the subscriber has timed out, he/she must re-subscribe to the service.

AP-2500 Authentication Methods

6. Configure the **Amount Paid** field, if desired. The AP automatically fills in this field after a successful credit card purchase.
 7. Configure the optional **User Alias** fields, if desired. These are for notes only and do not have an impact on the authentication process.
 8. Configure the **Upstream** and **Downstream Bandwidth** limits for the user. The user's bandwidth is not limited if you leave this blank or set it to 0.
 9. Click **OK** to add the subscriber.
 10. Click the back arrow button to return to the **Authorized Subscriber List** screen.
- To edit a subscriber entry, click **Edit**, make the necessary changes to the Subscriber's profile and click **OK**. Click the back arrow button to return to the **Authorized Subscriber List** screen.
 - To delete a subscriber, click **Edit** and set **Status** to **Destroy**. Click **OK** to remove the entry and click the back button to return to the previous screen.



NOTE

An active subscriber will immediately lose his/her access to the Internet if the subscriber's entry is deleted from the Authorized Subscribers Table. You can also delete subscribers from **Monitor > Subscribers**. See [Current Subscribers Table](#).

34. Reboot the AP so all of your changes take effect. The easiest way to reboot is to click **Commands > Reboot > OK**.
35. Launch a computer that has a wireless card installed. Note that the card's wireless settings must match the AP's Wireless Interface settings to communicate (see [Interfaces](#) for more information on the wireless settings). If the card can successfully communicate with the AP, the subscriber should now be able to create an account or logon to the Internet.

Internal Authentication with RADIUS

In this configuration, the AP-2500 provides all of the authentication services described in [Internal Authentication](#), but it also communicates with a Remote Authentication Dial-In User Service (RADIUS) server on the network to determine if a user is valid. RADIUS is an authentication and accounting protocol that is used by many ISPs. The RADIUS server maintains a large central list of subscribers and their attributes (such as the maximum bandwidth allowed for a specific customer) that it communicates back to the AP-2500. The RADIUS server can also perform accounting functions to record a user's login activity to facilitate billing.

RADIUS is a proven carrier-class protocol to perform accurate time and volume-based billing. The RADIUS protocols are defined in RFCs 2865 (Authentication) and 2866 (Accounting). These RFCs are available at <http://www.rfc-editor.org/>.

➡ NOTE

In RADIUS terminology, the AP is referred to as a **RADIUS Client** or as a **Network Access Server (NAS)**.

Authentication Procedure

The following diagram illustrates how a client is authenticated when the AP's RADIUS client is enabled.

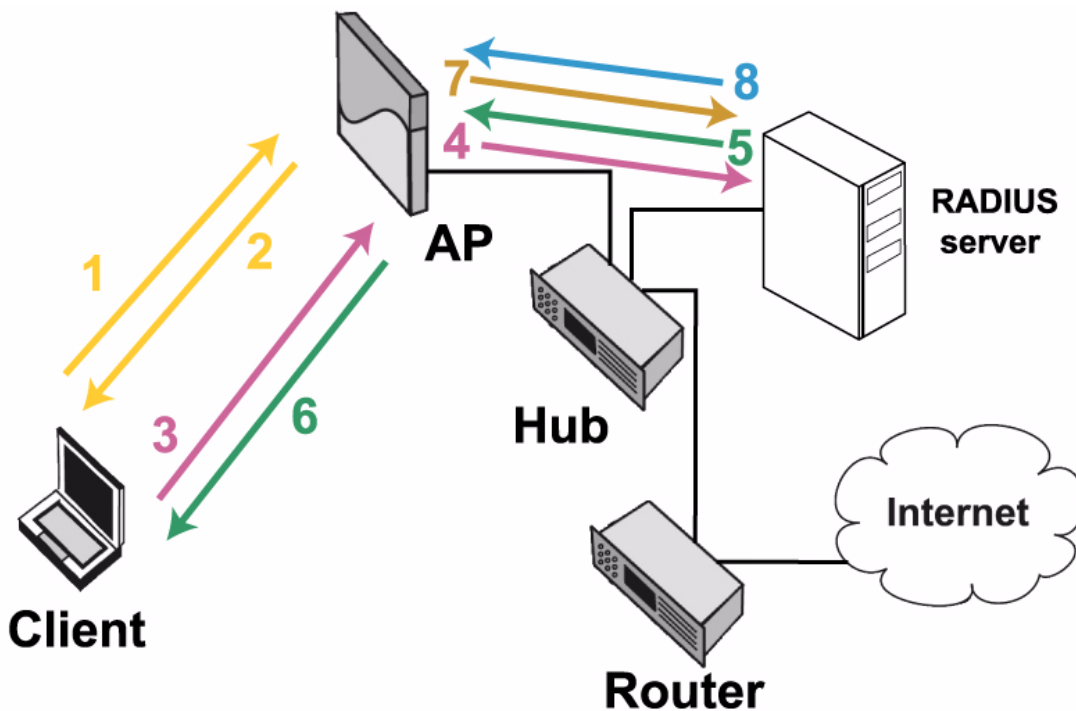


Figure 3-3 Internal Authentication with RADIUS

1. Client connects to AP and launches Web browser. The AP adds the client to its [Current Subscribers Table](#) with State set to "Pending".
2. AP redirects client to the AP's internal login page or to a [Portal Page](#).
 - The AP redirects the customer when it receives an HTTP request from the customer's browser.
 - If the browser's default home page is loaded in the browser's cache, the customer may not be redirected to the login screen. But the customer will be redirected the first time he tries to access a new Web site.
 - The customer must try to access a valid Web site to call up the login screen. Entering an unreachable URL or invalid Web address will not bring up the login screen.
 - Customers who try to access e-mail first will not have a connection. Customers need to login via a Web browser first.

AP-2500 Authentication Methods

3. Client sends AP its login credentials (User name/password or MAC address).
4. AP checks its [Authorized Subscribers](#) Table. If the client is not listed, the AP forwards the authentication request to the RADIUS server.
5. The RADIUS server authenticates the user based on the client's login credentials and notifies AP of successful authentication.
6. AP changes the client's State to "Valid" in its [Current Subscribers Table](#) and redirects the client to the requested Web page or to the site specified by Home Page Redirection settings.
7. AP sends an accounting "start" message to the RADIUS server.
 - This assumes that RADIUS accounting is enabled.
 - Note that you can use the same server for RADIUS authentication and accounting or two different RADIUS servers: one for authentication and one for accounting).
8. RADIUS server sends an acknowledgment back to the AP that the accounting message was successfully received.
 - This assumes that RADIUS accounting is enabled.
 - In addition to sending an accounting "start" message when a subscriber logs in, the AP also sends an accounting "stop" message when the subscriber logs out or times out. Also, the AP can send interim accounting messages at a specified interval (but not less than every two minutes).

Notes Concerning RADIUS

- Subscribers authenticated by RADIUS can logout of their Internet sessions in one of three ways:
 - By clicking the **Logout** button found on the ICC (if enabled).
 - See [Information and Control Console \(ICC\)](#) and [Potential End User Issues](#) for more information and a list of known issues.
 - By typing **http://1.1.1.1/** in their Web browser.
 - By clicking a link to **http://1.1.1.1/** that you add to a custom [Portal Page](#).
- Subscribers authenticated by RADIUS are logged out automatically in one of two ways:
 - **Idle timer** expires.
 - **Session timer** expires.

(These two timers are RADIUS attributes that you can configure for the subscribers in your RADIUS database. See [RADIUS Messages and RADIUS Attributes](#) for details.)
- See [RADIUS](#) for more information on the AP's RADIUS implementation.

Configuration Instructions

The configuration instructions are divided into two topics:

- [Install and Configure RADIUS](#)
- [Configure the AP-2500](#)

Install and Configure RADIUS

Before you install or configure the AP-2500, you should first install and configure the RADIUS server on your network. There are multiple RADIUS applications available. Popular RADIUS servers include Microsoft's Internet Authentication Service (IAS), Funk's Steel-belted RADIUS, and Lucent Navis RADIUS. Microsoft's IAS server is included with Windows 2000 Server.

Since your specific installation and configuration steps will vary based on the RADIUS server you select, the following instructions are only an overview of the process. Refer to the documentation included with your RADIUS server for detailed instructions.



NOTE

Contact your RADIUS server manufacturer if you have problems configuring the server or have problems using RADIUS authentication and/or accounting.

AP-2500 Authentication Methods

1. Install the RADIUS application on your network server, if necessary.
 - IAS is included with Windows 2000 Server. If you want to install IAS, follow these steps:
 1. Click **Start > Control Panel**.
 2. Double-click the **Add/Remove Programs** icon.
 3. Click the **Add/Remove Windows Components** option.
 4. Double-click the **Networking Services** option.
 5. Place a check mark next to the **Internet Authentication Service** option.
 6. Click **OK**.
 7. Click **Next** and follow the on-screen instructions to install IAS.
 8. You may be prompted to insert your Windows 2000 installation CD during the installation process.
2. Add the AP as a Client within the RADIUS server application.
 - Follow these steps if using IAS:
 1. Click **Start > Programs > Administrative Tools > Internet Authentication Service**.
 2. Right-click the **Clients** folder (located in the navigation tree) and choose **New Client** from the drop-down menu.
 3. Enter a name for the AP in the **Friendly Name** field and click **Next**. (Protocol should be set to **RADIUS**.)
 4. Enter the AP's IP address in the **Client address (IP or DNS):** field.
 5. Set the **Client-vendor:** to **RADIUS Standard**.
 6. Enter a **Shared Secret** in the field provided. Re-enter the password in the **Confirm shared secret:** field.
 - Make a note of the Shared Secret you entered. You will also need to configure the AP to use the same Shared Secret.
 7. Click **Finish**.
3. Add your list of users to the RADIUS database. When using the AP-2500, you can authenticate subscribers using the following credentials:
 - **User-Input** (that is, User Name and Password)
 - **MAC-MAC** (Enter the MAC address as both the user name and the password)
 - **MAC-Key** (Enter the MAC address as the user name and the AP/RADIUS **Shared Secret** as the password)
 - If using **MAC-MAC** or **MAC-Key**, enter the MAC address in the following format: 123456-7890ab (6 digits, a dash, final 6 digits).
 - The following steps describe how to configure your users if using IAS:
 1. Click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
 2. Click the **Users** folder (located in the navigation tree).
 3. Click **Action > New > User**.
 4. Follow the on-screen instructions to add a new user to the Active Directory (use one of the three formats above to configure the login name and password).
 5. Follow these steps for each user you added to the database:
 - Right-click the user's entry and click **Properties**.
 - Click the **Dial-In** tab.
 - Set **Remote Access Permission (Dial-In or VPN):** to **Allow access**.
 - Set **Callback options:** to **No Callback**.
 - Click **OK**.
 6. Click **Action > New > Group**.
 7. Enter a **Group** name.
 8. Set **Group Scope** to **Global**.
 9. Set **Group Type** to **Security**.
 10. Click **OK**.
 11. Right-click the new group you created and select **Properties** from the drop-down list.
 12. Click the **Members** tab.
 13. Click **Add**.
 14. Select the users you want to add to the Group and click **Add**.
 15. Click **OK** twice to return to main screen.

AP-2500 Authentication Methods

16. Return to the **Internet Authentication Services** window and right-click the **Remote Access Policies** entry in the navigation tree.
 17. Select **New Remote Access Policy** from the drop-down menu.
 18. Enter a **Policy friendly name** in the field provided and click **Next**.
 19. Click **Add**.
 20. Select **Windows-Groups** from the list and click **Add**.
 21. Click **Add** again to view the list of groups.
 22. Select the group that contains your AP's subscribers and click **Add**.
 23. Click **OK** twice and click **Next**.
 24. Select **Grant remote access permission** and click **Next**.
 25. Click **Edit Profile** and select the **Authentication** tab.
 26. Select **Unencrypted Authentication (PAP, SPAP)** as the authentication method and click **OK**.
 27. Click **Finish**.
4. The AP-2500 supports four Vendor-Specific Attributes (VSAs) designed by Nomadix, Inc. Configure the following VSAs, if desired:



NOTE

See [RADIUS Messages and RADIUS Attributes](#) for the list of all supported RADIUS attributes.

- **Nomadix-Bw-Up** (*attribute number: 1; format: integer/decimal; attribute value: enter upstream bandwidth*)
— This attribute value (in Kbps) restricts the speed at which subscriber uploads are performed.
- **Nomadix-Bw-Down** (*attribute number: 2; format: integer/decimal; attribute value: enter downstream bandwidth*)
— This attribute value (in Kbps) restricts the speed at which subscriber downloads are performed.
- **Nomadix-URL-Redirection** (*attribute number: 3; format: string; attribute value: enter redirection URL*)
— This attribute allows the administrator to redirect the user to a page of the administrator's choice after every successful login.
— Enter the redirection URL in the following format: **http://www.myhotspot.com/**
- **Nomadix-IP-Upsell** (*attribute number: 4; format: integer/decimal; attribute value: enter 1 to enable*)
— This attribute allows the user to receive a public address from a DHCP pool (typically relay DHCP server) when the AP has the IP-Upsell feature enabled.
- The following steps describe how to configure the VSAs if using IAS:



NOTE

With Windows 2000 IAS, you configure RADIUS attributes based on Remote Access Policies. In other words, you must apply the same attributes to all Group members identified by a particular policy. Other RADIUS applications allow you to assign attributes on a per-user basis.

1. Click **Start > Programs > Administrative Tools > Internet Authentication Services**.
2. Click the **Remote Access Policies** entry in the navigation tree.
3. Right-click the policy for which you want to enable one or more VSAs and choose **Properties**.
4. Click **Edit Profile... > Advanced** and click **Add**.
5. Select **Vendor Specific** and click **Add**.
6. Click **Add** and select **Enter Vendor Code**.
7. Enter **3309** in the **Vendor code:** field and select **Yes, it conforms**.
8. Click **Configure Attribute** and enter the **Vendor-assigned attribute number**, **Attribute format** (string or decimal) and the **Attribute value** (see above to determine what settings to use).
9. Click **OK** twice.
10. Enter additional VSAs or click **OK** to continue.
11. Click **Close**.
12. Click **OK** twice.

AP-2500 Authentication Methods

Configure the AP-2500

After you have installed and configured your RADIUS server, you need to configure your AP to communicate with the RADIUS server and provide internal authentication. Follow these steps:

1. Configure the AP-2500 to use its Internal Web Server for authentication. See [Internal Authentication > Configuration Instructions](#) for step-by-step instructions.
2. If not already open, access the AP's Web browser interface.
3. Click **Configure > Security > RADIUS**.
 - The **RADIUS Access** screen is divided into four parts:
 - RADIUS Servers
 - Retransmission Options
 - ISP Account Creation
 - Options
4. Configure the **RADIUS Server** options.
 - **Authentication:**
 1. Place a check mark in the **Enable Servers** box.
 2. Enter the server's IP address in the **Primary Server IP Address** field OR enter the server's DNS name in the **Primary Server DNS Name** field. Use either identifier but not both.
 3. Enter the **Primary Server Port** number.
 - This port must match the RADIUS Authentication port supported by your RADIUS program. Most RADIUS servers use port 1812 (the default setting) for Authentication. However, Funk Steel-belted RADIUS uses port 1645.
 4. Enter the Shared Secret for the AP and RADIUS server in **Primary Server Secret Key** field. This is the same Shared Secret that you used when you added the AP as one of the RADIUS server's clients.
 5. Repeat the above procedure for the **Secondary Server** parameters if you have a back-up RADIUS server.
 - **Accounting:**
 1. Place a check mark in the **Enable Servers** box.
 2. Enter the server's IP address in the **Primary Server IP Address** field OR enter the server's DNS name in the **Primary Server DNS Name** field. Use either identifier but not both.
 3. Enter the **Primary Server Port** number.
 - This port must match the RADIUS Accounting port supported by your RADIUS program. Most RADIUS servers use port 1813 (the default setting) for Accounting. However, Funk Steel-belted RADIUS uses port 1646.
 4. Enter the Shared Secret for the AP and RADIUS server in **Primary Server Secret Key** field. This is the same Shared Secret that you used when you added the AP as one of the RADIUS server's clients.
 5. Repeat the above procedure for the **Secondary Server** parameters if you have a back-up RADIUS server.



NOTE

A single RADIUS server can perform both Authentication and Accounting. Alternatively, you can use separate servers for each function.

AP-2500 Authentication Methods

5. Configure the **Retransmission Options**.
 - Select a **Retransmission Method**. This option is only valid if you have configured settings for a Secondary Server.
 - **Failover**: The AP make multiple attempts to reach the Primary Server. If the Primary Server fails to respond (after the specified number of Retransmission Attempts), the AP falls over to the Secondary Server.
 - **Round-Robin**: The AP first attempts to reach the Primary Server. If the Primary Server fails to respond, the AP tries the Secondary Server. If the Secondary Server fails to respond, the AP again tries the Primary Server.
 - Enter the number of seconds between retransmission attempts in the **Retransmission Frequency** field.
 - Enter the number of retransmission attempts (per server) in the **Retransmission Attempts** field.
 - Enter the number of seconds after which a retransmission attempt times out in the **Retransmission Timeouts** field.
6. Configure the **ISP Account Creation** options (if applicable).
 - This option is provided for demo purposes. It acts as a portal page HTTP redirection to allow new users to sign up for service with an ISP.
 - You can specify a URL to redirect new customers (i.e., a portal page) and a URL to containing an account creation form, and the ISP Server's IP Address.



NOTE

If you enable this feature for demo purposes, you must also add the ISP Server's IP address to the [Passthrough IP Table](#).

7. Configure the miscellaneous RADIUS **Options**.
 - Select a **User Name/Password Type**. This option determines what credentials the RADIUS server uses to authenticate subscribers.
 - **User-Input** (that is, User Name and Password)
 - **MAC-MAC** (The wireless card's MAC address is used as both the user name and the password)
 - **MAC-Key** (The wireless card's MAC address is the user name and the AP/RADIUS **Shared Secret** is the password)
 - If using **MAC-MAC** or **MAC-Key**, enter the MAC address in the following format: 123456-7890ab (6 digits, a dash, final 6 digits).
 - Place a check mark in the **Enable RADIUS Profile Caching** box, if desired.
 - When enabled, the AP maintains the user's information in the [Current Subscribers Table](#) (**State: Pending**) after a user logs out or times out. If the user attempts to re-connect, he can access the service again without being prompted to re-enter his user name and password.
 - This option uses the subscriber card's MAC address to re-validate the user. For security reasons, you may not want to enable this option. It is theoretically possible that an unauthorized individual could capture the user's MAC address and use it to spoof the AP to connect to the network when the actual user is not logged in.
 - Place a check mark in the **Enable URL Redirection** box if you configured the Nomadix-URL-Redirection VSA.
 - Place a check mark in the **Send Framed IP** box if you want to include the IP address assigned to the client in the messages sent to RADIUS server.
 - You can use this parameter to help identify the IP address assigned to clients in the RADIUS accounting logs. If using IP Upsell, you can also see how many clients are using public IP addresses.
 - Place a check mark in the **Send NAS Identifier** box if you want to include the AP's **NAS Identifier** in the messages sent to the RADIUS server.
 - Configure the **NAS Identifier** if you enabled **Send NAS Identifier**. (In RADIUS terminology, the AP is the NAS or Network Access Server.)
 - You can use this parameter to differentiate between multiple APs in the RADIUS accounting logs.
 - Also, the RADIUS server can alter a user's access policy depending on the NAS identifier. For example, the maximum session time could be reduced if the NAS identifier is "restaurant" instead of "library."

AP-2500 Authentication Methods

- Place a check mark in the **Send NAS Port Type** box if you want to include the port type in the messages sent to the RADIUS server.
 - Set the **NAS Port Type** to **19** if you enabled **Send NAS Port Type**.
 - Port Type 19 corresponds to a connection made over an IEEE 802.11 Wireless network. See RFC 2865 for details (the RFC is available at <http://www.rfc-editor.org/>).
 - You can also use NAS Port Type to establish different access policies. For example, in a cyber café there could be two access types: wired and wireless and you could charge more for access from a wired computer that is part of your network infrastructure.
 - Set the **Default User Idle Timeout**.
 - The AP times out users who are inactive for the specified number of seconds.
 - The AP only uses this parameter if the Idle-Timeout attribute is not set or if it specifies an amount of time that is greater than this setting. See [RADIUS Messages](#) and [RADIUS Attributes](#) for details.
 - When set to 0, a user never times out (assuming that the Idle-Timeout attribute is not set).
8. Click **OK**.
 9. Click **PublicSpace > AAA > Internal**.
 10. Confirm that there is check mark next to the **Enable User Names** box if you are authenticating users based on User name/Password.
 11. Place a check mark in the **Enable Smart Client** box if you are a partner with a hotspot aggregator, such as Boingo, iPass, or GRIC, and you want to support subscribers who have the aggregator's Smart Client application installed on their computers. In this case, the RADIUS settings you configured should point to the aggregator's RADIUS servers. See [Smart Client](#) for details.
 12. Click **OK** if you made any changes.
 13. Reboot the AP.

External Authentication

The External Web Server (EWS) interface was designed for customers who want to develop and use their own content. It allows for more customization than if using the Internal Web Server (IWS). By using an EWS (External Web Server) you can authenticate subscribers externally; the EWS is responsible for interacting with accounting or authorizing services. You can use this authentication method if you have an existing authentication and billing system place and you want to integrate the AP into that solution.

The AP uses XML (eXtensible Markup Language) to communicate with an External Web Server and obtain information about current users. XML is a newer, more elegant way to use custom web content. XML is an open standard that is tied closely into the HTML standard. XML is maintained by the World Wide Web Consortium (W3C). See <http://www.w3.org/> for more information on W3C and XML. Also, see RFC 3470 at <http://www.rfc-editor.org/>.

The AP can accept commands that follow the XML specification detailed in [XML Interface Specification](#). The XML interface allows the AP to accept and process these XML commands received from an external source. XML commands are sent from the external source (External Web Server) in the form of an encoded query string. The AP parses the query string, executes the commands specified by the string, and returns data to the system that initiated the command request.

Authentication Procedure

The following diagram illustrates how a client is authenticated when the process is handled by an EWS.

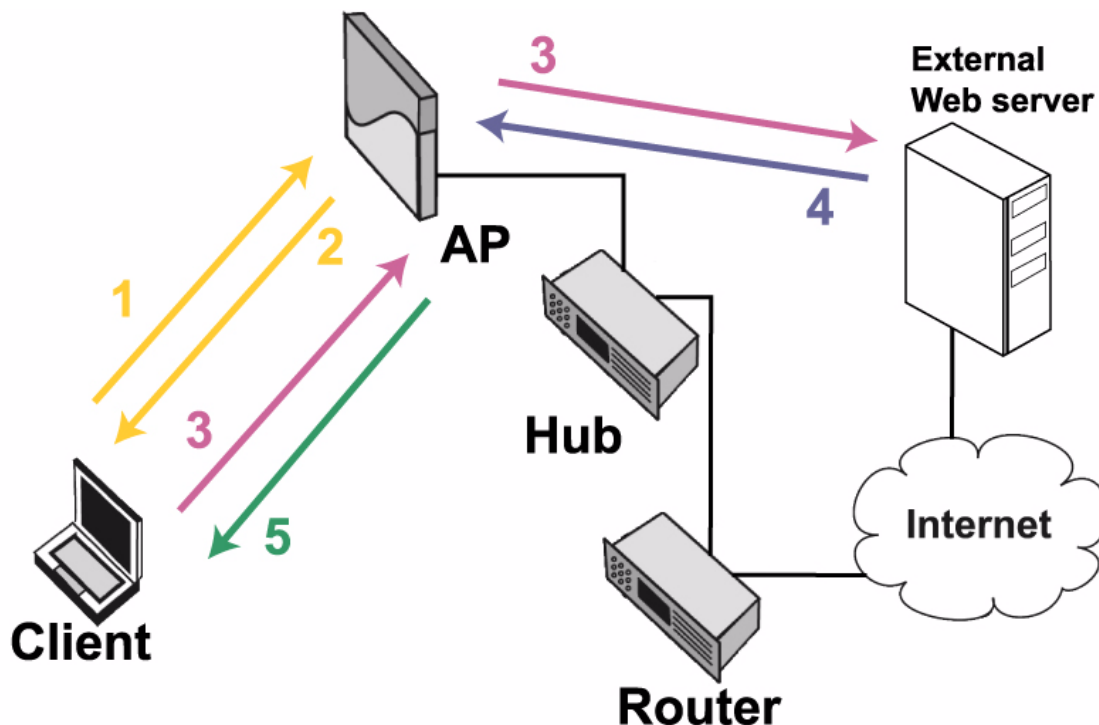


Figure 3-4 External Authentication

1. Client connects to AP and launches Web browser. The AP adds the client to its [Current Subscribers Table](#) with State set to "Pending".
2. AP redirects client to the **External Login Page URL** located on the EWS (the EWS can be located on the AP's local network or on the Internet).
 - The AP redirects the customer when it receives an HTTP request from the customer's browser.
 - If the browser's default home page is loaded in the browser's cache, the customer may not be redirected to the external login page. But the customer will be redirected the first time he tries to access a new Web site.

AP-2500 Authentication Methods

- The customer must try to access a valid Web site to initiate a redirect. Entering an unreachable URL or invalid Web address will not initiate a redirect to the External portal page.
- Customers who try to access e-mail first will not have a connection. Customers need to login via a Web browser first.
- 3. Client sends its login credentials (User name/password) to the EWS (by way of the AP).
- 4. EWS authenticates the user based on the client's login credentials and notifies AP of successful authentication using XML commands (USER_ADD and UPDATE_CACHE).
- 5. AP performs the following tasks:
 - Adds client to its [Authorized Subscribers](#) Table based on the settings received from the EWS.
 - Updates the user's State to "Valid" within its [Current Subscribers Table](#).
 - Redirects client to requested Web page or site specified by Home Page Redirection settings.

Configuration Instructions

The configuration instructions are divided into two topics:

- [Setup your External Web Server](#)
- [Configure the AP-2500](#)

Setup your External Web Server

Before configuring the AP to communicate with an EWS, you need to set up your Web server and determine how the AP-2500 can integrate into your existing billing system (if applicable). You will also need to write the appropriate scripts to communicate user information to the AP using XML and design a login page for your users that interfaces with your external authentication service and communicates information back to the AP. See the [XML Interface Specification](#) for more information.



NOTE

This configuration is intended for advanced users who have some background in Web design. You may want to consider implementing either [Internal Authentication](#) or [Internal Authentication with RADIUS](#) if you do not have experience working with XML.

Configure the AP-2500

Follow these steps to configure the AP to communicate with an External Web Server:

1. Configure the AP-2500's basic settings. This includes the AP's IP address, System parameters, and management passwords. See [Basic Configuration](#) for details.
2. If not already open, access the AP's Web browser interface. (See [Logging into the Web Interface](#) for instructions.)
3. Click **Configure > Network > DHCP Server** to configure the AP's [DHCP Server](#) settings. The default setting should be suitable for most networks.
 - By default, the AP is configured to provide IP addresses to subscribers in the range of 10.0.0.12 to 10.0.0.36 with a 255.255.255.0 subnet mask. This is a private IP range. In most configurations, you should have assigned the AP a public IP address (that is, an address valid on the Internet). Using the default settings, the AP performs Network Address Translation (NAT) to provide Internet access to its clients. See [Dynamic Address Translation \(DAT\)](#) for more information on NAT.
 - You should change the default address range if it conflicts with the settings of another DHCP server on your network. Also, before modifying the AP's address pool, confirm that there is not another DHCP server on the network already serving addresses from this particular address range.
 - You can disable the AP's DHCP server if there is another DHCP server that you want to use instead. See [Disabling the AP's DHCP Server](#) for details.
4. Configure **IP Upsell**, if desired. See [IP Upsell](#) for details.
 - In general, it costs more to obtain public IP addresses from your ISP due to limited availability. If you have a pool of public IP addresses that you can distribute, you can offer standard customers less expensive private IP addresses and premium customers public IP addresses. This concept is known as "IP Upsell".

AP-2500 Authentication Methods

- Some applications require a public IP address to function properly over the Internet (such as certain VPN applications, on-line gaming, and Web hosting). Customers who require a public IP address may be willing to a premium for this service.
 - The subscriber's wireless card must be configured to obtain an IP address from a DHCP server to use the IP Upsell feature (that is, this feature doesn't work if the subscriber's computer is assigned a static IP address).
5. Click **OK** to save your changes to the DHCP Server settings.
 6. Click the **DNS Server** tab to configure Domain Name Service (DNS) settings. This information may already be provided for you if the AP's **IP Address Type** is **Dynamic**.
 - Enter a **DNS Host Name** for the AP. The default setting is suitable for most configurations unless you have multiple APs and want to assign each one a different Host Name.
 - Enter the **DNS Domain** name. This name is provided by your ISP or network administrator.
 - Enter up to three DNS Server IP addresses in the fields provided. You must configure at least the Primary DNS Server IP address. These IP addresses should be provided by your ISP or network administrator.



NOTE

The AP must be configured with a valid DNS Server IP address to function correctly. If you are setting up a demo with this equipment, the AP must be able to communicate with a valid DNS server before it will function as expected. If you do not configure DNS, then all Internet locations must be in IP address format, including HTTP requests from subscribers.

7. Click **OK** to save your changes to the DNS Server settings.
8. Click the **Public Space** button.
9. Click the **AAA** tab.
10. Place a check mark in the **Enable AAA Services** box.
11. Place a check mark in the **Enable XML Interface** box.
 - You must enable XML support if you plan to use an External Web Server.
12. Enter the IP address of your External Web Server in the **XML Sender IP Address** field.
13. Set **Authorization Method** to **External**.
14. Click **OK**.
15. Click the **External** tab.
16. Enter the IP address of the External Web Server in the **IP Address** field.
17. Enter the location of the subscriber login page in the **External Login Page URL** field.
 - The AP will redirect unauthenticated customers to this page.
 - Be sure to enter your External Web Server's IP address in the **Passthrough IP Table** so unauthenticated users can access the external login page.
 - If your external login page is a secure HTTPS page, configure the AAA Passthrough Port 443 to allow secure traffic to pass through from unauthenticated clients. See [Passthrough AAA Port](#).



NOTE

The **Secret Key** parameter is reserved for future use. You can leave the parameter set to default value.

18. Click **OK**.
19. Click the **Passthrough** tab.
20. Enter the IP Address of the External Web Server in the **Passthrough IP Table**.
21. Enter the DNS Names for all of the Web sites that you want to include in your "walled garden" in the **Passthrough DNS Table** (if applicable).
 - A "walled garden" is a list of Web site that your customers can access for free without logging into the AP.
 - If you want to provide free access to customers for a limited number of sites, you can include links to these pages on your custom login page.
 - You can enter a single World Wide Web address (such as **www.yahoo.com**) or you can enter Domain Names (such as ***.yahoo.com**). Entering the Domain Name provides users will full access to the specified Domain's Web sites. For example, if you enter **www.yahoo.com** in the DNS Passthrough Table, customers will not be able to access sites such as **http://finance.yahoo.com** as part of the walled garden.

AP-2500 Authentication Methods

22. Click the **AAA Port** tab and configure the AAA Passthrough Port settings, if applicable. For example, if you are redirecting customers to a secure HTTPS page, you should set the AAA Passthrough Port for port 443. See [Passthrough AAA Port](#).
23. If you plan to limit subscriber bandwidth or offer multiple access plans based on bandwidth speeds, click the **Bandwidth Mgmt** tab to notify the AP of its bandwidth settings.
 - These parameters correspond to the AP's connection to the Ethernet and the Internet. Based on these settings, the AP determines the speed of its Internet connection. The AP uses this information when making bandwidth allocations to subscribers.
 - Do not set uplink or downlink speed to 0; this will disable access to the unit over the Ethernet.
 - The upper limit for uplink or downlink speed is 100,000 Kbps (100 Mbps). This is the maximum speed at which the AP can connect to the Ethernet network. In reality, the uplink and downlink speeds will depend upon the speed of your hotspot's Internet connection (for example, T1 or DSL) and the speed of the wireless cards installed in the AP (up to 54 Mbps if using 802.11a).
 - By default, Bandwidth Management is enabled and uplink and downlink speeds are set to 1500 Kbps.
24. If you want to redirect outgoing e-mail traffic to your Simple Mail Transfer Protocol (SMTP) server, click the **SMTP** tab and configure the SMTP Redirection settings. See [SMTP Redirection](#).
 - Most SMTP servers only transmit e-mail messages that originate from local traffic to prevent illegal use of a mail server by spammers, hackers, and other unauthorized individuals. Therefore, most of your subscribers will be unable to send email messages unless you enable SMTP Redirection.
 - When SMTP Redirection is enabled, all outgoing mail traffic is redirected to the SMTP server you specify in the **SMTP Server IP** field (this field is based on IP address and not DNS name). This will allow subscribers to send emails without changing any of the server settings in their email program. Typically, this will be your local mail server (if you have one) or your ISP's mail server.
 - If you want all outgoing mail traffic redirected to the specified server, enable both the **Misconfigured** and **Properly Configured** options. **Misconfigured** refers to subscribers whose email settings are incompatible with the AP-2500's Internet settings (in other words, these email settings may work on the subscriber's home or office network but they won't work in the hotspot); **Properly Configured** refers to subscribers whose e-mail settings should work on the hotspot network so you do not necessarily need to redirect these messages to your own server. If you want properly configured subscribers to send mail without being redirected, enable only the **Misconfigured** option. In general, Proxim recommends that you enable both options. Also, you should never enable **Properly Configured** and disable **Misconfigured** (this combination defeats the purpose of SMTP Redirection).
25. If you want to redirect the user to a specified URL following successful authentication, click **HPR** and configure the Home Page Redirection options. See [Home Page Redirection \(HPR\)](#) for details.
26. If you want a customized banner applet to appear on subscriber's browser screens, click **ICC** and configure the Information and Control Console options. See [Information and Control Console \(ICC\)](#) for details, caveats, and customization instructions.
 - The ICC is a Java applet that is pushed to your customer's Web browsers. You can customize the ICC's banners and buttons to promote partner Web sites.
27. If you want to block subscribers from accessing certain Web sites, click **URLFilter** and configure the URL Filtering options. See [URL Filtering](#) for details.
28. Reboot the AP.

4

Network Parameters

In This Chapter

This chapter describes all of the network operating parameters that can be configured using the Access Point's Web browser interface (that is, the parameters accessible after clicking the **Configure** button).

- **System:** Configure specific system information such as system name and contact information.
- **Network:** Configure IP settings, DHCP server, DNS servers, and VLAN.
- **Interfaces:** Configure the Access Point's interfaces: Wireless (A and/or B) and Ethernet.
- **Management:** Configure the Access Point's management Passwords, IP Access Table, Services, and NTP.
- **Filtering:** Configure Ethernet Protocol filters and Static MAC Address filters.
- **Alarms:** Configure the Alarm (SNMP Trap) Groups and the Alarm Host Table.
- **Bridge:** Configure the AP to operate in bridge mode so it behaves like a traditional access point (for troubleshooting purposes).
- **Security:** Configure security features such as MAC Access Control, RADIUS parameters, WEP Encryption, and VPN.

NOTE

See [Logging into the Web Interface](#) for instructions on how to access the AP's Web browser interface.

System

You can configure and view the following parameters within the **System Configuration** screen:

- **Name:** The name assigned to the AP-2500.
- **Location:** The location where the AP-2500 is installed.
- **Contact Name:** The name of the person responsible for the AP-2500.
- **Contact Email:** The e-mail address of the person responsible for the AP-2500.
- **Contact Phone:** The telephone number of the person responsible for the AP-2500.
- **Object ID:** This is a read-only field that displays the Access Point's MIB definition; this information is useful if you are managing the AP-2500 using SNMP.
- **Ethernet MAC Address:** This is a read-only field that displays the unique MAC (Media Access Control) address for the Access Point's Ethernet interface. The MAC address is assigned at the factory.
- **Descriptor:** This is a read-only field that reports the Access Point's name, serial number, current image software version, and current bootloader software version.
- **Up Time:** This is a read-only field that displays how long the Access Point has been running since its last reboot.

Network Parameters

Network

The Network category contains four sub-categories.

- [IP Configuration](#)
- [DHCP Server](#)
- [DNS Server](#)
- [VLAN](#)

IP Configuration

You can configure and view the following parameters within the **IP Configuration** screen (see [Set the Access Point's IP Address](#) for step-by-step instructions):

- **IP Address Assignment Type:** Set this parameter to **Dynamic** to configure the Access Point as a Dynamic Host Configuration Protocol (DHCP) client; the Access Point will obtain IP settings from a network DHCP server automatically during boot-up. If you do not have a DHCP server or if you want to manually configure the Access Point's IP settings, set this parameter to **Static**.



NOTE

For best results, Proxim recommends that you assign the AP-2500 a static public IP address that is routable on the Internet. If you use a dynamic IP address, some of the Public Space features may not work properly if the IP address changes at a later date.

- **IP Address:** The Access Point's IP address. When IP Address Assignment Type is set to Dynamic, this field is read-only and reports the unit's current IP address. When shipped from the factory or reset to factory settings, the Access Point defaults to a static IP address of 10.0.0.10.
- **Subnet Mask:** The Access Point's subnet mask. When IP Address Assignment Type is set to Dynamic, this field is read-only and reports the unit's current subnet mask. When shipped from the factory or reset to factory settings, the Access Point defaults to a subnet mask of 255.255.255.0.
- **Gateway IP Address:** The IP address of the Access Point's gateway. When IP Address Assignment Type is set to Dynamic, this field is read-only and reports the IP address of the unit's gateway (as assigned by the DHCP server). When shipped from the factory or reset to factory settings, the Access Point defaults to a gateway IP address of 10.0.0.1.

DHCP Server

The AP-2500 acts as a Dynamic Host Configuration Protocol (DHCP) server for subscribers whose wireless cards are configured as DHCP clients. This is the typical configuration for most hotspot subscribers.

By default, the AP is configured to provide IP addresses to subscribers in the range of 10.0.0.12 to 10.0.0.36 with a 255.255.255.0 subnet mask. This is a private IP range. In most configurations, you should have assigned the AP a public IP address (that is, an address that is valid on the Internet). Using the default settings, the AP performs Network Address Translation (NAT) to provide Internet access to its clients. See [Dynamic Address Translation \(DAT\)](#) for more information on NAT.

In general, you should not need to change the default DHCP Server parameters unless one of the following conditions apply:

- Your network already uses the 10.0.0.0 network and there is another DHCP server on the network already serving these addresses to devices.
- You want a DHCP server (other than the AP) to assign addresses to your subscribers.
- You have more than 25 subscribers and need to increase the number of addresses in the DHCP pool.
- You want the AP to serve clients from a pool of public IP addresses you have obtained from your ISP.
- You want to enable IP Upsell.

Network Parameters

Overview of DHCP Server Parameters

You can configure and view the following parameters within the **DHCP Server Configuration** screen:

- **Enable DHCP Server:** Place a check mark in the box provided to enable DHCP Server functionality. Remove the check mark if you do not want the AP to act as a DHCP server.
- **DHCP Server Type:** Specifies the type of IP address the AP will provide to clients: **public** or **private**. By default, the AP serves addresses in the 10.0.0.0 range, which are private addresses, so this field is set to private.
- **DHCP Server IP Address:** The IP address that the AP will use to communicate with subscribers.
- **DHCP Server Subnet Mask:** The subnet mask that the AP will assign to subscribers.
- **Pool Start IP Address:** Specifies the first IP address in the address range that the AP will use to provide addresses to subscribers.
- **Pool End IP Address:** Specifies the last IP address in the address range that the AP will use to provide addresses to subscribers.
- **Lease Time:** Specifies in minutes the length of time for which the subscriber's IP address lease is valid. A subscriber must renew its address lease after the lease time elapses. The default is 1440 minutes. This parameter supports a range from 0 (lease never expires) to 65536 minutes.
- **Enable DHCP IP Upsell:** Place a check mark in the box provided to enable this feature. See [IP Upsell](#) for details.
- **Enable DHCP Relay:** Place a check mark in this box if you unchecked the **Enable DHCP Server** option and you want subscribers to obtain IP addresses from a DHCP server other than the AP. This parameter is automatically enabled when IP Upsell is enabled.
- **Relay Type:** Specifies the type of addresses that the DHCP Relay server will serve to subscribers: public or private. Set this parameter to **public** when enabling IP Upsell.
- **DHCP Relay Agent IP:** If the DHCP Relay Server is on the same IP network as the AP, leave this parameter set to 0.0.0.0. If the DHCP Relay Server and the AP are on different IP networks, set this parameter so it matches the AP's IP address.
- **DHCP Relay Server IP:** Enter the IP address of the remote DHCP server which will provide IP addresses to subscribers. The AP will forward DHCP requests from these clients to the DHCP Relay server.

NOTE

You must reboot the Access Point before changes to any of these DHCP server parameters take effect.

The DHCP server in the access point allows for dynamic IP address assignment to wireless clients only.

Note: Changes to these parameters require access point reboot in order to take effect.

To enable IP Upsell feature, DHCP Server and DHCP Relay needs to be enabled and if DHCP Server is public then DHCP relay needs to be private or if DHCP Server is private then DHCP relay needs to be public.

Enable DHCP Server	<input checked="" type="checkbox"/>	
DHCP Server Type	<input checked="" type="radio"/> Private	<input type="radio"/> Public
DHCP Server IP Address	<input type="text" value="10.0.0.4"/>	
DHCP Server Subnet Mask	<input type="text" value="255.255.255.0"/>	
Pool Start IP Address	<input type="text" value="10.0.0.12"/>	
Pool End IP Address	<input type="text" value="10.0.0.36"/>	
Lease Time (minutes)	<input type="text" value="1440"/>	
Enable DHCP IP Upsell	<input type="checkbox"/>	
Enable DHCP Relay	<input type="checkbox"/>	
Relay Type	<input type="radio"/> Private	<input checked="" type="radio"/> Public
DHCP Relay Agent IP	<input type="text" value="0.0.0.0"/>	
DHCP Relay Server IP	<input type="text" value="0.0.0.0"/>	

OK Cancel

Figure 4-1 DHCP Server Configuration Screen

Configuring the AP to Serve Public IP Addresses

If you have a pool of public IP addresses and do not want the AP to perform NAT for subscribers who have DHCP client support enabled, follow these steps (note that this is not a typical configuration for the device):

1. Login to the Web interface.
2. Click **Configure > Network > DHCP Server**.
3. Set the **DHCP Server Type** to **public**.
4. Set the **DHCP Server IP Address** to the AP's IP address.
5. Configure the **DHCP Server Subnet Mask** and the range of IP addresses as required by your network.
6. Edit the **Lease Time**, if necessary.
7. Click **OK**.
8. Reboot the AP.

Disabling the AP's DHCP Server

If you want a DHCP server other than the AP to assign IP addresses to your subscribers, you can disable the AP's DHCP Server functionality and configure the DHCP Relay Server settings (which specify the DHCP server you want to use). Follow these steps:

1. Login to the Web interface.
2. Click **Configure > Network > DHCP Server**.
3. Remove the check mark from the **Enable DHCP Server** box.
4. Place a check mark in the **Enable DHCP Relay** box.
 - The **Enable DHCP IP Upsell** box should remain unchecked.

Network Parameters

5. In the **Relay Type** field, select the type of addresses your DHCP server will assign to subscribers: **Public** or **Private**.
6. In the **DHCP Relay Server IP** field, enter the IP address of your DHCP server.
7. Configure the **DHCP Relay Agent IP** as follows:
 - If the DHCP Relay Server is on the same IP network as the AP, enter **0.0.0.0** in this field.
 - If the DHCP Relay server is on a different IP network from the AP, enter the AP's IP address in this field.
8. Click **OK**.
9. Reboot the AP.

IP Upsell

The AP-2500 will provide a DHCP lease for any subscriber with DHCP client enabled. Typically this will be a private IP address assigned from the AP's primary DHCP address pool. However, some customers may require a public, routable IP address to support all of their Internet programs. Some applications require a public IP address to function properly over the Internet (such as certain VPN applications, on-line gaming, and Web hosting). Customers who require a public IP address may be willing to pay a premium for this service.

Using the AP's DHCP Relay option, you can provide two address pools to your customers: one private and one public. If you have a pool of public IP addresses that you can distribute, you can offer standard customers less expensive private IP addresses and premium customers public IP addresses. This concept is known as **IP Upsell**. A subscriber can select the type of IP address when signing up for a billing plan or using the ICC (see [Information and Control Console \(ICC\)](#) for details).

Note that a subscriber needs to have DHCP enabled to use the IP Upsell feature. This option will be unavailable to customers whose computers have a static IP address. Also, a subscriber may need to reboot his/her computer for the new public address to take effect (the ICC automatically informs the user of this requirement).

How IP Upsell Works

When a subscriber first connects to the AP, the AP provides a private DHCP lease from its primary pool. This lease has an expiration time of five minutes.

When the subscriber selects a billing plan that provides a public IP address, the AP forwards the subscriber's DHCP request to the specified DHCP Relay server.

If the subscriber is logging in through a RADIUS account, then the Nomadix-IP-Upsell Vendor Specific Attribute (VSA) can be added to subscriber's RADIUS user information and passed back to the AP. This would still have the same sequence for IP lease handout (that is, private address for five minutes and then public after authentication).

After selecting a plan (private or public address), the client's lease time is determined by the DHCP server that assigned it an address (if the AP assigns it an address from its primary pool, the lease time is determined by the configured **Lease Time** parameter).

Enabling IP Upsell

Follow these steps to enable IP Upsell:

1. Login to the AP's Web browser interface.
2. Click **Configure > Network > DHCP Server**.
3. Update the AP's primary DHCP settings (that is, all options above the **Enable DHCP IP Upsell** option) if necessary so that it distributes private IP addresses from this pool.
4. Place a check mark in the **Enable DHCP IP Upsell** box. A check mark will appear in the **Enable DHCP Relay** box automatically.
5. Set the **Relay Type** to **Public**.
6. In the **DHCP Relay Server IP** field, enter the IP address of the DHCP server that will provide public IP addresses to the subscribers who select a service plan which includes a public IP address.
7. Configure the **DHCP Relay Agent IP** as follows:
 - If the DHCP Relay Server is on the same IP network as the AP, enter **0.0.0.0** in this field.
 - If the DHCP Relay server is on a different IP network from the AP, enter the AP's IP address in this field.
8. Click **OK**.
9. Click the **Subscriber** button.
10. Click the **Billing** tab.

Network Parameters

The screenshot shows the Proxim Network Parameters configuration window. The 'Network' tab is selected, and the 'DHCP Server' sub-tab is active. The interface includes a left sidebar with buttons for Status, Configure, Monitor, Commands, PublicSpace, Subscriber, Help, and Exit. The main content area contains the following settings:

- Enable DHCP Server:** ☒
- DHCP Server Type:** ☒ Private ☐ Public
- DHCP Server IP Address:** 10.0.0.4
- DHCP Server Subnet Mask:** 255.255.255.0
- Pool Start IP Address:** 10.0.0.12
- Pool End IP Address:** 10.0.0.36
- Lease Time (minutes):** 1440
- Enable DHCP IP Upsell:** ☒
- Enable DHCP Relay:** ☒
- Relay Type:** ☐ Private ☒ Public
- DHCP Relay Agent IP:** 0.0.0.0
- DHCP Relay Server IP:** 205.23.45.3

At the bottom are 'OK' and 'Cancel' buttons. A note at the top states: 'The DHCP server in the access point allows for dynamic IP address assignment to wireless clients only.' Another note mentions: 'Note: Changes to these parameters require access point reboot in order to take effect.' A third note explains: 'To enable IP Upsell feature, DHCP Server and DHCP Relay needs to be enabled and if DHCP Server is public then DHCP relay needs to be private or if DHCP Server is private then DHCP relay needs to be public.'

Figure 4-2 Enabling IP Upsell

11. Configure the billing plans that you want to offer.
 - At least one plan should offer private IP addresses and at least one plan should offer public IP addresses (you can configure up to six different billing plans).
 - See [Billing Options for Subscribers](#) for detailed instructions on how to configure the billing plans.
12. Reboot the AP.

Notes Concerning IP Upsell

- A subscriber needs to have DHCP enabled to use the IP Upsell feature. This option will be unavailable to customers whose computers have a static IP address.
- If you use internal authentication, configure at least one billing plan to offer private IP addresses and one billing plan to offer public IP address so that the IP Upsell feature is available to subscribers. See [Billing Options for Subscribers](#) for more information.
- If you use RADIUS, add the Vendor Specific Attribute for IP Upsell to your subscribers' RADIUS profiles. See [Install and Configure RADIUS](#) and [RADIUS Messages and RADIUS Attributes](#) for details.
- If you want to let customer dynamically upgrade from a private IP billing to a public IP plan, enable ICC. See [Information and Control Console \(ICC\)](#) for details.

Network Parameters

- If you use external authentication, you can add an **IP_Type** attribute to the **User_Add** XML command and specify the address type (public or private), as shown in the following example:

```
<USG COMMAND="USER_ADD" MAC_ADDR="0050da554787">
<USER_NAME>johndoe</USER_NAME>
<PASSWORD ENCRYPT="FALSE">doededoe</PASSWORD>
<EXPIRY_TIME UNITS="SECONDS">3600</EXPIRY_TIME>
<ROOM_NUMBER></ROOM_NUMBER>
<PAYMENT_METHOD>CREDIT_CARD</PAYMENT_METHOD>
</IP_Type>PUBLIC</IP_Type>
<CONFIRMATION></CONFIRMATION>
<PAYMENT>4.95</PAYMENT>
</USG>
```

See [XML Interface Specification](#) for more information.

DNS Server

The Domain Name System (DNS) maps a host name to its IP address on the Internet. The AP redirects DNS resolution requests to a local DNS server on behalf of subscribers. The AP must have valid DNS settings and be able to communicate with a DNS server to provide Internet access to customers.



NOTE

If you are setting up a demo with this equipment, the AP must be able to communicate with a valid DNS server before it will function as expected. If you do not configure DNS, then all Internet locations must be in IP address format, including HTTP requests from subscribers.

The screenshot shows the 'DNS Server' configuration page. At the top, there are tabs for 'Filtering', 'Alarms', 'Bridge', 'Security', 'System', 'Network' (selected), 'Interfaces', and 'Management'. Under the 'Network' tab, there are sub-tabs for 'IP Configuration', 'DHCP Server', 'DNS Server' (selected), and 'VLAN'. The main content area contains the following text and fields:

The DNS server in the access point allows address resolution for both wireless clients and wired hosts.

Note: Changes to these parameters require access point reboot in order to take effect.

DNS Host Name	hotspotap
DNS Domain	nrodw01.md.comcast.net
Primary DNS Server IP Address	68.48.0.6
Secondary DNS Server IP Address	68.48.0.5
Tertiary DNS Server IP Address	0.0.0.0

At the bottom, there are 'OK' and 'Cancel' buttons.

Figure 4-3 DNS Server Configuration Screen

Follow these steps to configure the DNS Server settings:

1. Login to the Web interface.
2. Click **Configure > Network > DNS Server**.
3. Enter a **DNS Host Name** for the AP. The default Host Name should be suitable for most configurations unless you have multiple APs and want to assign each one a different Host Name.

Network Parameters

4. Enter the **DNS Domain** name. This name is provided by your ISP or network administrator.
5. Enter up to three DNS Server IP addresses in the fields provided. You must configure at least the Primary DNS Server IP address. These IP addresses should be provided by your ISP or network administrator.
6. Click **OK**.
7. Reboot the AP.

VLAN

Virtual Local Area Networks (VLANs) are logical groupings of network resources. Defined by software settings, VLAN resources appear (to clients) to be in the same room, no matter where they are attached on the physical LAN segment. They simplify traffic flow between clients and their frequently-used or restricted resources.

VLANs now extend as far as the access point signal reaches; clients can connect from anywhere in the broadcast area. The broadcast area is defined by the network name configured for the wireless card on the access point device.

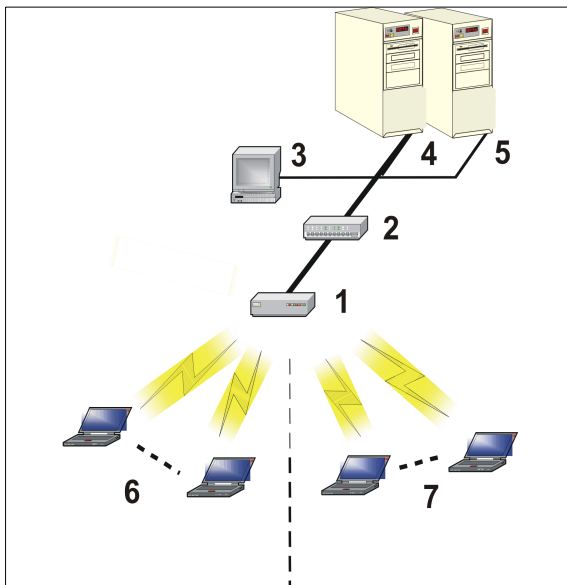
AP-2500 devices are fully VLAN-ready; however, by default VLAN support is disabled. Before enabling VLAN support, certain network settings should be configured, and network resources such as a VLAN-aware switch, a RADIUS server, and possibly a DHCP server should be available.

Once enabled, VLANs are used to more conveniently, efficiently, and easily manage your network.

- Manage adds, moves, and changes from a single point of contact
- Define and monitor groups
- Reduce broadcast and multicast traffic to unnecessary destinations
 - Improve network performance and reduce latency
- Increase security
 - Secure network restricts members to resources on their own workgroup
 - Clients roam without compromising security

Typical VLAN Configurations

VLANs collect and distribute data through the cards installed in the AP-2500. An Ethernet port on the access point typically connects a wireless cell to a wired backbone. They communicate across a VLAN-capable switch that reviews packet headers and directs traffic to the appropriate ports. In the example below, a RADIUS server authenticates traffic on the Ethernet network and a DHCP server manages IP addresses.



In this figure, the numbered items correspond to the following components:

1. VLAN-enabled AP
2. VLAN-aware switch (IEEE 802.1Q uplink)
3. AP-2500 management via wired host (SNMP, Web interface or CLI)
4. DHCP Server
5. RADIUS Server
6. VLAN 1 (Wireless Card A)
7. VLAN 2 (Wireless Card B)

Figure 4-4 Components of a typical VLAN

VLAN Workgroups and Traffic Management

Traditional, dual-slot access point devices that are not VLAN-capable typically broadcast and multicast traffic over both wireless cells. This process wastes wireless bandwidth and degrades throughput performance. In comparison, the dual-slot, VLAN-capable AP-2500 device is designed to efficiently manage delivery of broadcast, multicast, and unicast traffic to wireless clients.

The AP-2500 device assigns clients to one of two VLANs designated by a network name. First, each one of the wireless cards in the AP-2500 device is configured with a unique network name and an 802.1Q-compliant VLAN identifier. Each card represents a VLAN.

Each network client is then assigned one of the two wireless NIC network names. The AP-2500 device matches packets transmitted or received to a network name with the associated VLAN. Traffic received by a VLAN is only sent on the wireless card associated with that same VLAN. This eliminates unnecessary traffic on the wireless LAN, conserving bandwidth and maximizing throughput.

Traffic Management

In addition to enhancing wireless traffic management, the VLAN-capable AP-2500 device supports easy assignment of wireless users to workgroups. In a typical scenario, each user VLAN represents a workgroup; for example, one VLAN could be used for an EMPLOYEE workgroup and the other, for a GUEST workgroup.

In this scenario, the AP-2500 device would assign every packet it accepted to a VLAN. Each packet would then be identified as EMPLOYEE or GUEST, depending on which wireless NIC received it. The AP-2500 device would insert VLAN headers or “tags” with identifiers into the packets transmitted on the wired backbone to a network switch.

Finally, the switch would be configured to route packets from the EMPLOYEE workgroup to the appropriate corporate resources such as printers and servers. Packets from the GUEST workgroup transmitted on the same network as packets from the EMPLOYEE workgroup, could, in contrast, be restricted to a gateway that allowed access to only the Internet. A member of the GUEST workgroup could send and receive e-mail and access the Internet, but would be prevented from accessing servers or hosts on the local corporate network.

Typical User VLAN Configurations

VLANs segment network traffic into workgroups, which enable you to limit broadcast and multicast traffic. Workgroups enable clients from different VLANs to access different resources using the same network infrastructure. Clients using the same physical network are limited to those resources available to their workgroup. The three primary scenarios for use of the VLAN support feature are detailed as follows.

- Scenario 1: Setting Up Independent VLAN Workgroups (“Tagged” User VLANs)
- Scenario 2: Setting Up Independent VLAN Workgroups (Tagged & Untagged User VLANs)
- Scenario 3: Setting Up One VLAN Workgroup (One Tagged VLAN)

Setting Up Independent VLAN Workgroups

When VLAN support is enabled, the AP-2500 tags all traffic received from wireless clients with a header identifying each packet as belonging to one VLAN workgroup, or another.

To configure this scenario, set up two different workgroups with separate VLAN Identifiers (IDs).

- VLAN ID for Wireless card in Slot A = a number between 1 and 4094 (per the IEEE 802.1Q standard)
- VLAN ID for Wireless card in Slot B = a number between 1 and 4094



NOTE

The number configured for the wireless card in Slot A must be different than the number configured for the wireless card in Slot B.

Figure 4-5 VLAN Configuration Screen (Wireless A and Wireless Tagged with Different VLAN IDs)

1. Login to the Web interface.
2. Click **Configure > Interfaces > Wireless A**.
3. Set the SSID for card A.
4. Click the **Wireless B** tab.
5. Set the SSID for card B (this should be different from the SSID for card A).
6. Click **Network > VLAN**.
7. Set a unique VLAN ID for each wireless card (enter a value between 1 and 4094)
8. Place a check mark in the **Enable VLAN Protocol** box.
9. Click **OK**.
10. Configure the wireless client with one of the two Network Names based on VLAN membership.

Setting Up Independent VLAN Workgroups

The VLAN-capable AP-2500 supports configuration of both “tagged” and “untagged” user VLANs.

A “tagged” user VLAN is created when a VLAN ID between 1 and 4094 (per the 802.1Q standard) is configured for one of the wireless cards and VLAN is enabled. The AP-2500 applies a VLAN header to tag traffic from wireless clients (members of a “tagged” VLAN) and transmits the traffic as appropriate, on either the wired or wireless backbone.

An “untagged” User VLAN is created when a VLAN ID of 0 is configured for one of the wireless cards and VLAN is enabled. Traffic received from wireless clients (members of an “untagged” VLAN) is transmitted as appropriate, on either the wired or wireless backbone. “Untagged” User VLANs enable VLANs to coexist on networks with non-VLAN capable devices such as legacy servers.

To configure this scenario, set up only one workgroup by configuring one VLAN and untagged traffic:

- VLAN ID for Wireless card in Slot A = 0 or a number between 1 and 4094
- VLAN ID for Wireless card in Slot B = 0 or a number between 1 and 4094



NOTE

Either the wireless card in Slot A or the wireless card in Slot B must be set to 0 to support this configuration.

Figure 4-6 VLAN Configuration Screen (Slot A tagged; Slot B untagged)

1. Login to the Web interface.
2. Click **Configure** > **Interfaces** > **Wireless A**.
3. Set the SSID for card A.
4. Click the **Wireless B** tab.
5. Set the SSID for card B (this should be different from the SSID for card A).
6. Click **Network** > **VLAN**.
7. Set the **VLAN ID** for one card to 0.
8. Set the **VLAN ID** for the other card to a value between 1 and 4094.
9. Place a check mark in the **Enable VLAN Protocol** box.
10. Click **OK**.
11. Configure the wireless client with one of the two Network Names based on VLAN membership.

Setting Up a Single VLAN Workgroup

The VLAN feature enables all wireless clients that access the network through the same AP-2500, to be configured as members of the same VLAN. In this scenario, each wireless card is configured with the same VLAN ID. The same VLAN header or tag is then applied to all traffic received from wireless clients and transmitted on the wired or wireless backbone. All wireless clients become members of the same VLAN.

To configure this scenario, set up one, large workgroup:

- VLAN ID for Wireless card in Slot A = a number between 1 and 4094 (the same number as Slot B)
- VLAN ID for Wireless card in Slot B = a number between 1 and 4094 (the same number as Slot A)

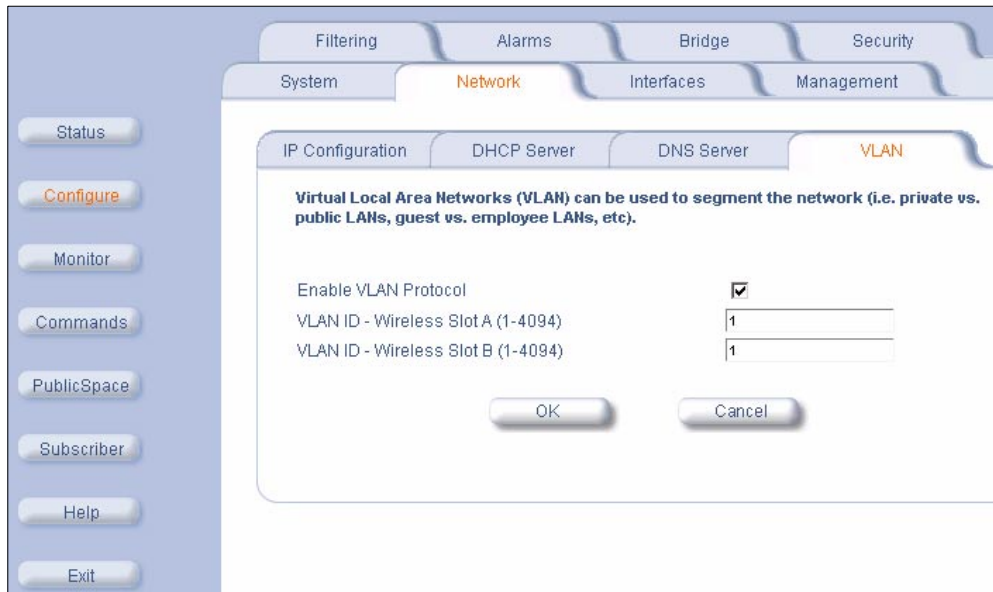


Figure 4-7 VLAN Configuration Screen (Wireless A and Wireless B Use Same VLAN ID)

1. Login to the Web interface.
2. Click **Configure** > **Interfaces** > **Wireless A**.
3. Set the SSID for card A.
4. Click the **Wireless B** tab.
5. Set the SSID for card B (this can be the same SSID as card A).
6. Click **Network** > **VLAN**.
7. Set the **VLAN ID** for the card in Slot A to a value between 1 and 4094.
8. Set the **VLAN ID** for the card in Slot B to the same value configured for the card in Slot A.
9. Place a check mark in the **Enable VLAN Protocol** box.
10. Click **OK**.
11. Configure the wireless client with one of the two Network Names based on VLAN membership.

Interfaces

From the **Interfaces** tab, you configure the Access Point's radio and Ethernet settings. Refer to the Wireless parameters below that correspond to your Access Point's radio type(s).

- [Wireless \(802.11a\)](#)
- [Wireless \(802.11b\)](#)
- [Ethernet](#)

Depending on the type of wireless PC Card installed in the AP-2500, the configuration options will be different. Some parameters are the same for 802.11a and 802.11b cards. Others are unique to each card type.

You can setup an AP-2500 unit using the following combinations of wireless cards:

1. single 802.11a card with the attached antenna adapter
2. single 802.11b card
3. two 802.11b cards (one in each slot)
4. one 802.11a card with attached antenna and one 802.11b card



NOTE

Wireless - A and **Wireless - B** refer to a card's location in the AP (Slot A or Slot B) and not to the available radio standards (that is, 802.11a or 802.11b).

Network Parameters

Wireless (802.11a)

You can configure and view the following parameters within the **Wireless Interface Configuration** screen for an 802.11a radio:



NOTE

You must reboot the Access Point before any changes to these parameters take effect.

- **Physical Interface Type:** This field reports: "802.11a (OFDM 5 GHz)." OFDM stands for Orthogonal Frequency Division Multiplexing; this is the name for the radio technology used by 802.11a devices.
- **MAC Address:** This is a read-only field that displays the unique MAC (Media Access Control) address for the Access Point's wireless interface. The MAC address is assigned at the factory.
- **Network Name (SSID):** Enter a Network Name (between 1 and 31 characters long) for the wireless network. You must configure each wireless client to use this name as well. See [Configure Network Names for the Wireless Interfaces](#) for more information.
- **Auto Channel Select:** The AP-2500 scans the area for other Access Points and selects a free or relatively unused communication channel. This helps prevent interference problems and increases network performance. By default this feature is enabled. Note that you cannot disable Auto Channel Select for 802.11a products in Europe (see [Dynamic Frequency Selection \(DFS\)](#) for details).
- **Frequency Channel:** When Auto Channel Select is enabled, this field is read-only and displays the Access Point's current operating Channel. When Auto Channel Select is disabled, you can specify the Access Point's Channel. If you decide to manually set the unit's Channel, ensure that nearby devices do not use the same frequency. Available Channels vary based on regulatory domain. See [802.11a Channel Frequencies](#). Note that you cannot manually set the channel for 802.11a products in Europe (see [Dynamic Frequency Selection \(DFS\)](#) for details).
- **Transmit Rate:** Use the drop-down menu to select a specific transmit rate for the 802.11a radio. Choose between 6, 9, 12, 18, 24, 36, 48, 54 Mbits/s, and Auto Fallback. Auto Fallback is the default setting; it allows the AP to select the best transmit rate based on the cell size.

Filtering Alarms Bridge Security

System Network **Interfaces** Management

Wireless - A Wireless - B Ethernet

Wireless interface properties determine the characteristics of the wireless medium as well as how wireless clients will communicate with the access point.

Note: Changes to these parameters require access point reboot in order to take effect.

Physical Interface Type	802.11a (OFDM 5 GHz)
MAC Address	00:30:F1:48:2A:0D
Network Name (SSID)	My Wireless Network A
Enable Auto Channel Select	<input checked="" type="checkbox"/>
Frequency Channel	52 - 5.260 GHz
Transmit Rate	Auto Fallback
DTIM Period (1-65535 sec)	1
RTS/CTS Medium Reservation (2347=off)	2347

OK Cancel

Figure 4-8 Wireless Interface Configuration Screen (802.11a)

- **DTIM Period:** The Deferred Traffic Indicator Map (DTIM) is used with clients that have power management enabled. DTIM should be left at 1, the default value, if any clients have power management enabled. This parameter supports a range between 1 and 65535.
- **RTS/CTS Medium Reservation:** This parameter affects message flow control and should not be changed under normal circumstances. Range is 0 to 2347. When set to a value between 0 and 2347, the Access Point uses the RTS/CTS mechanism for packets that are the specified size or greater. When set to 2347 (the default setting), RTS/CTS is disabled. See [RTS/CTS Medium Reservation](#) for more information.

Dynamic Frequency Selection (DFS)

802.11a devices sold in Europe use a technique called Dynamic Frequency Selection (DFS) to automatically select an operating channel. During boot-up, the AP scans the available frequency and selects a channel that is free of interference. If the AP subsequently detects interference on its channel, it automatically reboots and selects another channel that is free of interference.

DFS only applies to 802.11a devices used in Europe (i.e., units whose regulatory domain is set to ETSI). The European Telecommunications Standard Institute (ETSI) requires that 802.11a devices use DFS to prevent interference with radar systems and other devices that already occupy the 5 GHz band.

If you are using an AP with a 5 GHz upgrade kit in Europe, keep in mind the following:

- DFS is not a configurable parameter. It is always enabled and cannot be disabled.
- You cannot manually select the device's operating channel; you must let DFS select the channel.
- You cannot configure the **Auto Channel Select** option. Within the Web browser interface, this option always appears enabled.

RTS/CTS Medium Reservation

The 802.11 standard supports optional RTS/CTS communication based on packet size. Without RTS/CTS, a sending radio listens to see if another radio is already using the medium before transmitting a data packet. If the medium is free, the sending radio transmits its packet. However, there is no guarantee that another radio is not transmitting a packet at the same time, causing a collision. This typically occurs when there are hidden nodes (clients that can communicate with the Access Point but are out of range of each other) in very large cells.

When RTS/CTS occurs, the sending radio first transmits a Request to Send (RTS) packet to confirm that the medium is clear. When the receiving radio successfully receives the RTS packet, it transmits back a Clear to Send (CTS) packet to the sending radio. When the sending radio receives the CTS packet, it sends the data packet to the receiving radio. The RTS and CTS packets contain a reservation time to notify other radios (including hidden nodes) that the medium is in use for a specified period. This helps to minimize collisions. While RTS/CTS adds overhead to the radio network, it is particularly useful for large packets that take longer to resend after a collision occurs.

RTS/CTS Medium Reservation is an advanced parameter and supports a range between 0 and 2347 bytes. When set to 2347 (the default setting), the RTS/CTS mechanism is disabled. When set to 0, the RTS/CTS mechanism is used for all packets. When set to a value between 0 and 2347, the Access Point uses the RTS/CTS mechanism for packets that are the specified size or greater. You should not need to enable this parameter for most networks unless you suspect that the wireless cell contains hidden nodes.

Wireless (802.11b)

You can configure and view the following parameters within the **Wireless Interface Configuration** screen for an 802.11b radio:

NOTE

You must reboot the Access Point before any changes to these parameters take effect.

- **Physical Interface Type:** This field reports: "802.11b (DSSS 2.4 GHz)." DSSS stands for Direct Sequence Spread Spectrum; this is the name for the radio technology used by 802.11b devices.
- **MAC Address:** This is a read-only field that displays the unique MAC (Media Access Control) address for the Access Point's wireless interface. The MAC address is assigned at the factory.
- **Network Name (SSID):** Enter a Network Name (between 1 and 31 characters long) for the wireless network. You must configure each wireless client to use this name as well. See [Configure Network Names for the Wireless Interfaces](#) for more information.
- **Auto Channel Select:** The AP-2500 scans the area for other Access Points and selects a free or relatively unused communication channel. This helps prevent interference problems and increases network performance. By default this feature is enabled. However, if you are setting up a Wireless Distribution System (WDS), it must be disabled. See [Wireless Distribution System \(WDS\)](#) for more information.
- **Frequency Channel:** When Auto Channel Select is enabled, this field is read-only and displays the Access Point's current operating Channel. When Auto Channel Select is disabled, you can specify the Access Point's operating Channel. If you decide to manually set the unit's Channel, ensure that nearby devices do not use the same frequency (unless you are setting up a WDS). Available Channels vary based on regulatory domain. See [802.11b Channel Frequencies](#).

Network Parameters

- **Distance Between APs:** Set to **Large**, **Medium**, **Small**, **Microcell**, or **Minicell** depending on the site survey for your system. By default, this parameter is set to **Large**. The distance value is related to the **Multicast Rate** (described next). In general, a larger distance between APs means that your clients operate a slower data rates (on average). See [Distance Between APs](#) for more information.

Filtering Alarms Bridge Security
System Network **Interfaces** Management

Wireless - A **Wireless - B** Ethernet

Wireless interface properties determine the characteristics of the wireless medium as well as how wireless clients will communicate with the access point.

Warning: If WDS is enabled, then automatic channel selection should be disabled.

Note: Changes to these parameters require access point reboot in order to take effect.

Physical Interface Type 802.11b (DSSS 2.4 GHz)
MAC Address 00:02:2D:29:D7:98
Network Name (SSID) My Wireless Network B
Enable Auto Channel Select ☒
Frequency Channel 7 - 2.442 GHz
Distance Between APs Large
Multicast Rate 2 Mbit/Sec
DTIM Period (1-65535 sec) 1
RTS/CTS Medium Reservation (2347=off) 2347
Enable Interference Robustness ☐
Enable Closed System ☐
Enable Load Balancing ☒
Enable Medium Density Distribution ☐

OK Cancel

Wireless Distribution System (WDS)

WDS can be used to establish point-to-point (i.e. wireless backhaul) connections with other access points. This table is used to configure WDS partner access points.

Edit

Port Index	Partner MAC Address	Status
1	00:00:00:00:00:00	Disable
2	00:00:00:00:00:00	Disable
3	00:00:00:00:00:00	Disable
4	00:00:00:00:00:00	Disable
5	00:00:00:00:00:00	Disable
6	00:00:00:00:00:00	Disable

Figure 4-9 Wireless Interface Configuration Screen (802.11b)

Network Parameters

- **Multicast Rate:** Sets the rate at which Multicast messages are sent. This value is related to the Distance Between APs parameter (described previously). The table below displays the possible Multicast Rates based on the Distance between APs setting. By default, this parameter is set to 2 Mbits/sec. See [Multicast Rate](#) for more information.

Distance between APs	Multicast Rate
Large	1 and 2 Mbits/sec
Medium	1, 2, and 5.5 Mbits/sec
Small	1, 2, 5.5 and 11 Mbits/sec
Minicell	1, 2, 5.5 and 11 Mbits/sec
Microcell	1, 2, 5.5 and 11 Mbits/sec

- **DTIM Period:** The Deferred Traffic Indicator Map (DTIM) is used with clients that have power management enabled. DTIM should be left at 1, the default value, if any clients have power management enabled. This parameter supports a range between 1 and 65535.
- **RTS/CTS Medium Reservation:** This parameter affects message flow control and should not be changed under normal circumstances. Range is 0 to 2347. When set to a value between 0 and 2347, the Access Point uses the RTS/CTS mechanism for packets that are the specified size or greater. When set to 2347 (the default setting), RTS/CTS is disabled. See [RTS/CTS Medium Reservation](#) for more information.
- **Interference Robustness:** Enable this option if other electrical devices in the 2.4 GHz frequency band (such as a microwave oven or a cordless phone) may be interfering with the wireless signal. The AP will automatically fragment large packets into multiple smaller packets when interference is detected to increase the likelihood that the messages will be received in the presence of interference. The receiving radio reassembles the original packet once all fragments have been received. This option is disabled by default.
- **Closed System:** Check this box to allow only clients configured with the Access Point's specific Network Name to associate with the Access Point. When enabled, a client configured with the Network Name "ANY" cannot connect to the AP's 802.11b radio. This option is disabled by default.

⇒ NOTE

If you enable Closed System, you will need to inform your subscribers of the AP's Network Name; your subscribers will need to configure their client card's SSID to match this setting before gaining access to the network.

- **Load Balancing:** Enable this option so clients can evaluate which Access Point to associate with, based on current AP loads. This feature is enabled by default; it helps distribute the wireless load between APs. This feature is not available if you are using an ORiNOCO 802.11a/b ComboCard or a non-ORiNOCO client with the AP.
- **Medium Density Distribution:** When enabled, the Access Point automatically notifies wireless clients of its **Distance Between APs**, **Interference Robustness**, and **RTS/CTS Medium Reservation** settings. This feature is enabled by default and allows clients to automatically adopt the values used by its current Access Point (even if these values differ from the client's default values or from the values supported by other Access Points). Note that this feature is not available if you are using an ORiNOCO 802.11a/b ComboCard or a non-ORiNOCO client with the AP. Proxim recommends that you enable this parameter, particularly if your subscribers have ORiNOCO clients on your wireless network (leaving this parameter enabled should not adversely affect the performance of any ORiNOCO 802.11a/b ComboCards or non-ORiNOCO cards on your network).

Distance Between APs

Distance Between APs defines how far apart (physically) your APs are located, which in turn determines the size of your cell. Cells of different sizes have different capacities and, therefore, suit different applications. For instance, a typical office has many clients that require high bandwidth for complex, high-speed data processing. In contrast, a typical warehouse has a few forklifts requiring low bandwidth for simple transactions.

This parameter is particularly useful in roaming environments with traditional access points. However, this feature has limited applications with AP-2500 since the AP is designed for small to medium hotspot and offers only a few options for roaming (see [Limitations on Roaming](#)). Also, this feature is not available if you or your subscribers are using an ORiNOCO ComboCard or a non-ORiNOCO client with the AP.

The Distance Between Cells parameter supports five values: Large, Medium, Small, Minicell, and Microcell. You should set this parameter so you can provide your subscribers with the highest Multicast Rate for your environment. For example, if the AP provides strong coverage to wireless clients in all areas of your hotspot, you can set this value to Small. But if the connection is weak on the edges of your hotspot, set this value to Large.



CAUTION

You should conduct a Site Survey to determine the strength of the wireless connection on the borders of your hotspot. Contact your reseller for information on how to conduct a Site Survey.

Multicast Rate

The multicast rate determines the rate at which broadcast and multicast packets are transmitted by the Access Point to the wireless network. Stations that are closer to the Access Point can receive multicast packets at a faster data rate than stations that are farther away from the AP. Therefore, you should set the Multicast Rate based on the size of the Access Point's cell. For example, if the Access Point's cell is very small (e.g., Distance Between APs is set to Microcell), you can expect that all stations should be able to successfully receive multicast packets at 11 Mbits/sec so you can set Multicast Rate to 11 Mbits/sec. However, if the Access Point's cell is large, you need to accommodate stations that may not be able to receive multicast packets at the higher rates; in this case, you should set Multicast Rate to 1 or 2 Mbits/sec.

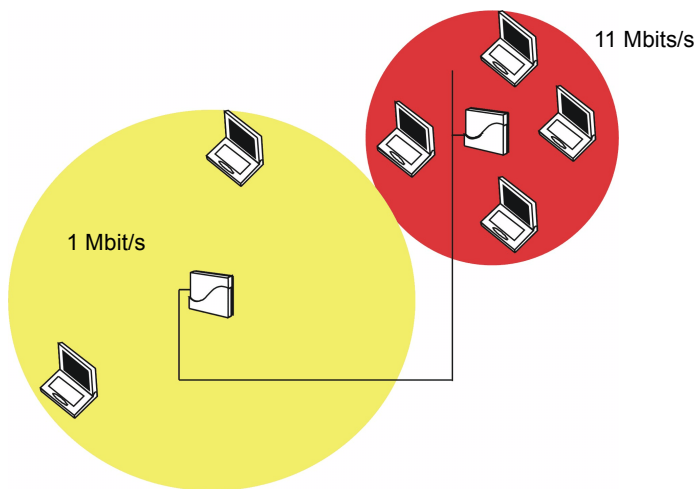


Figure 4-10 1 Mbits/s and 11 Mbits/s Multicast Rates



NOTE

The diagram above illustrates how the proximity of wireless clients can affect Multicast Rate. It is not meant to illustrate a roaming network.

There is an inter-dependent relationship between the Distance between APs and the Multicast Rate. In general, larger systems operate at a lower average transmit rate. The variation between Multicast Rate and Distance Between APs is presented in the following table:

	1.0 Mbit/s	2.0 Mbits/s	5.5 Mbits/s	11 Mbits/s
Large	yes	yes		
Medium	yes	yes	yes	
Small	yes	yes	yes	yes
Minicell	yes	yes	yes	yes
Microcell	yes	yes	yes	yes

The Distance Between APs **must be set before** the Multicast Rate, because when you select the Distance Between APs, the appropriate range of Multicast values automatically populates the drop-down menu. This feature is not available if you are using an ORiNOCO 802.11a/b ComboCard or a non-ORiNOCO client with the AP.

Wireless Distribution System (WDS)

A Wireless Distribution System (WDS) creates a link between two APs over their radio interfaces. This link relays traffic from one AP that does not have Ethernet connectivity to a second AP that has Ethernet connectivity.

Two AP-2500s cannot establish a WDS link with each other because each AP treats its wireless interfaces as subscriber interfaces only. A WDS link between AP-2500s would require that the AP accept backbone traffic over its wireless interface but that configuration is not currently supported (all backbone traffic must come from the Ethernet interface).

However, while you cannot establish a WDS link between two AP-2500s, you can establish a WDS link between an AP-2500 and up to six AP-2000 or AP-600b units. These links will work as long as the AP-2500 is the central AP that is connected to the Ethernet network, as illustrated in the following diagram:

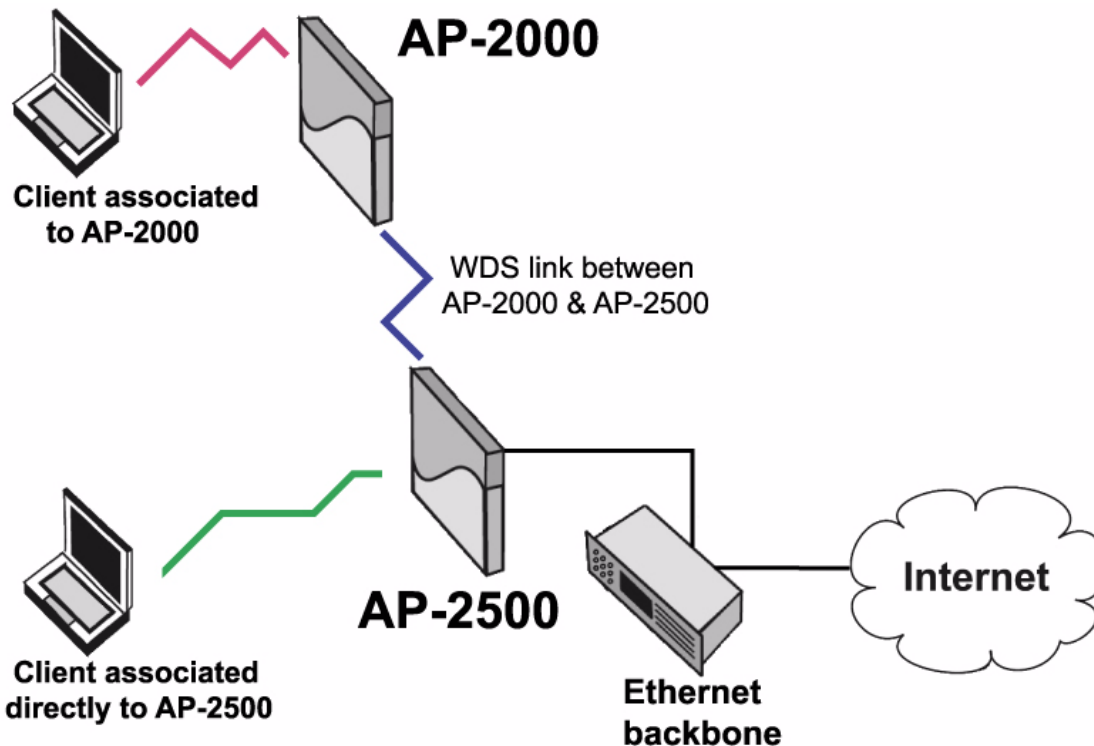


Figure 4-11 WDS Example

In the diagram above, the AP-2000 communicates with the AP-2500 over a WDS link (represented by the blue line). The client can connect to the AP-2500 through the AP-2000. This client will have Internet access and all of the same services as clients connected directly to the AP-2500 but the connection speed will be slower than if the client were communicating directly with the AP-2500.

Each WDS link is mapped to a logical WDS port on the AP. WDS ports behave like Ethernet ports rather than like standard wireless interfaces: on a BSS port, an Access Point learns by association and from frames; on a WDS or Ethernet port, an Access Point learns from frames only.

WDS Warnings

When setting up a WDS, keep in mind the following:

- You cannot create a WDS link between AP-2500s.
- When creating a WDS link between an AP-2500 and an AP-2000 or AP-600b, the AP-2500 must be connected to the Ethernet.
- WDS is not available with 802.11a radios.

Network Parameters

- The WDS link shares the communication bandwidth with the clients. Therefore, while the maximum data rate for the Access Point's cell is still 11 Mb/s/sec, client throughput will decrease when the WDS link is active. The connection over the link will be slower than if the client were communicating directly with the AP-2500.
- If there is no partner MAC address configured in the WDS table, the WDS port remains disabled.
- Each WDS port on an AP should have a unique partner MAC address. Do not enter the same MAC address twice in an AP's WDS port list.
- Each Access Point that is a member of the WDS must have the same Channel setting to communicate with each other.
- Auto Channel Selection must be disabled to create a WDS link.
- Each Access Point that is a member of the WDS must have the same WEP Encryption settings. Therefore, if you want to encrypt the WDS link, you must configure each Access Point to use WEP encryption and each Access Point must have the same Encryption Key (Key 1). See [Encryption](#).
- If your network does not support the Spanning Tree protocol, be careful to avoid creating network loops between APs. For example, creating a WDS link between two Access Points connected to the same Ethernet network will create a network loop. The AP-2500 does not support Spanning Tree.

WDS Setup Procedure

To setup a WDS link between an AP-2500 and an AP-2000 or AP-600b, follow the steps below for each AP that you wish to include in the Wireless Distribution System.

1. Confirm that the AP-2500 is connected to the Ethernet network in your proposed WDS topology.
2. Write down the MAC addresses of the APs that will be part of the WDS link.
3. Login to the AP-2500's Web browser interface.
4. Click **Configure > Interfaces > Wireless** (A or B) to open the configuration screen for the radio that will use WDS.
5. Disable **Auto Channel Select** if necessary.
6. Write down the **Frequency Channel** in use.
7. Scroll down to the **Wireless Distribution System** heading.
8. Click the **Edit** button to update the Wireless Distribution System (WDS) Table.
9. Enter the MAC address for the AP-2000 or AP-600b in one of the **Partner MAC Address** field of the **WDS Table Configuration** screen.
10. Set the **Status** of the device to **Enable**.
11. Click **OK**.

Wireless Distribution System (WDS)

WDS can be used to establish point-to-point (i.e. wireless backhaul) connections with other access points. This table is used to configure WDS partner access points.

Edit

Port Index	Partner MAC Address	Status
1	00:02:2D:12:34:56	Disable
2	00:00:00:00:00:00	Disable
3	00:00:00:00:00:00	Disable
4	00:00:00:00:00:00	Disable
5	00:00:00:00:00:00	Disable
6	00:00:00:00:00:00	Disable

Figure 4-12 WDS Configuration

12. Restart the AP.
13. Login to the AP-2000 or AP-600b's Web browser interface.

Network Parameters

14. Click **Configure > Interfaces > Wireless** (A or B, if applicable) to open the configuration screen for the radio that will use WDS.
15. Disable **Auto Channel Select** if necessary.
16. Change the **Frequency Channel** to match the AP-2500's Frequency Channel, if necessary.
17. Scroll down to the **Wireless Distribution System** heading.
18. Click the **Edit** button to update the Wireless Distribution System (WDS) Table.
19. Enter the MAC address for the AP-2500 in one of the **Partner MAC Address** field of the **WDS Table Configuration** screen.
20. Set the **Status** of the device to **Enable**.
21. Click **OK**.
22. Reboot the AP.

Ethernet

Select the desired speed and transmission mode from the drop-down menu. Half-duplex means that only one side can transmit at a time and full-duplex allows both sides to transmit. When set to auto-duplex, the AP negotiates with its switch or hub to automatically select the highest throughput option supported by both sides.

For best results, Proxim recommends that you configure the Ethernet setting to match the speed and transmission mode of the device the Access Point is connected to (such as a hub or switch). If in doubt, leave this setting at its default, **auto-speed-auto-duplex**. Choose between:

- 10 Mbit/s - half duplex, full duplex, or auto duplex
- 100 Mbit/s - half duplex or full duplex
- auto speed - half duplex or auto duplex



NOTE

See [Configure the Ethernet Interface](#) for step-by-step configuration instructions.

Management

The Management category contains four sub-categories.

- [Passwords](#)
- [IP Access Table](#)
- [Services](#)
- [Network Time Protocol \(NTP\)](#)



NOTE

You cannot configure an AP-2500 over its wireless interfaces. For security reasons, you can only configure the AP over its Ethernet port or its serial port.

Passwords

You can configure the following passwords:

- **SNMP Read Password:** The password for read access to the AP using SNMP. Enter a password in both the **Password** field and the **Confirm** field. The default password is "public".
- **SNMP Read/Write Password:** The password for read and write access to the AP using SNMP. Enter a password in both the **Password** field and the **Confirm** field. The default password is "public".
- **Telnet (CLI) Password:** The password for the CLI interface (via serial or Telnet). Enter a password in both the **Password** field and the **Confirm** field. The default password is "public".
- **HTTP (Web) Password:** The password for the Web browser interface. Enter a password in both the **Password** field and the **Confirm** field. The default password is "public".

Network Parameters

⇒ NOTE

For security purposes Proxim recommends changing ALL PASSWORDS from the default “public” immediately, to restrict access to your network devices to authorized personnel. If you lose or forget your password settings, you can always perform the [Reset to Factory Default Procedure](#).

IP Access Table

The IP Access Table limits management access over the Ethernet to the IP addresses or range of IP addresses specified in the table. This feature applies to all management options (SNMP, HTTP, and CLI) except for CLI management over the serial port.

Follow these steps to specify an authorized address range and enable this features:

1. Click **Configure > Management > IP Access Table**.
2. Click **Add**.
3. Enter the first IP address in the address range that will have access to the AP in the **Start IP Address** field.
4. Enter the last IP address in the address range in the **End IP Address** field.

⇒ NOTE

To specify a single IP address, enter the same address in both the **Start IP Address** and **End IP Address** fields.

5. Click **OK**.
6. Enter additional address ranges, if necessary.
7. Click the back button to return to the previous screen.
8. Place a check mark in the **Enable Access Control** box.
9. Click **OK**.

Once enabled, only those IP addresses that fall within the ranges specified in the IP Access Table will have access to the AP's management interfaces over the Ethernet network. To delete an entry, click **Edit** and select **Destroy** from the **Status** pull-down menu.

⇒ NOTE

You cannot enable Access Control unless one or more IP Address ranges exist in the IP Access Table. Also, if you remove all entries from the table, Access Control will be automatically disabled (that is, the AP will automatically remove the check mark from the **Enable Access Control** box).

Services

You can configure the following management services:

⇒ NOTE

You must reboot the Access Point if you change the HTTP Port or Telnet Port.

SNMP Settings

- **SNMP Interface Bitmask:** To allow management of the AP using SNMP, set this parameter to **Ethernet** (the default setting). You can also select **Disabled** to prevent a user from managing the AP via SNMP.

HTTP Access

- **HTTP Interface Bitmap:** To allow management of the AP using the Web browser interface, set this parameter to **Ethernet** (the default setting). You can also select **Disabled** to prevent Web-based management.
- **HTTP Port:** Configures the HTTP port from which you will manage the AP via the Web interface. By default, the HTTP port is 80.

Filtering Alarms Bridge Security

System Network Interfaces **Management**

Passwords IP Access Table **Services** NTP

This tab is used to configure SNMP, Telnet (CLI), and HTTP (web) parameters.

Note: Changes to these parameters require access point reboot in order to take effect.

SNMP Interface Bitmask All Interfaces

HTTP Interface Bitmask All Interfaces

HTTP Port 80

Telnet Interface Bitmask All Interfaces

Telnet Port Number 23

Telnet Login Idle Timeout (seconds) 30

Telnet Session Idle Timeout (seconds) 900

Serial Baud Rate 9600

Serial Flow Control None

Serial Data Bits 8

Serial Parity None

Serial Stop Bits 1

OK Cancel

Figure 4-13 Management Services Configuration Screen

Telnet Configuration Settings

- **Telnet Interface Bitmask:** To allow management of the AP using the CLI over a Telnet connection, set this parameter to **Ethernet** (the default setting). You can also select **Disabled** to prevent Telnet access.
- **Telnet Port:** The default port number for Telnet applications is 23. However, you can use this field if you want to change the Telnet port for security reasons (but your Telnet application also must support the new port number you select).
- **Login Idle Timeout (seconds):** Enter the number of seconds the system will wait for a login attempt. The AP terminates the session when it times out. The range is 1 to 300 seconds; the default is 30 seconds.
- **Session Idle Timeout (seconds):** Enter the number of seconds the system will wait during a session while there is no activity. The AP will terminate the session on timeout. The range is 1 to 36000 seconds; the default is 900 seconds.

Serial Configuration Settings

The serial port interface on the AP is enabled at all times. See [Using the Command Line Interface](#) for information on how to access the CLI interface via the serial port. You can configure and view following parameters:

- **Baud Rate:** Select the serial port speed (bits per second). Choose between 2400, 4800, 9600, 19200, 38400, or 57600; the default Baud Rate is 9600.
- **Flow Control:** Select either **None** (default) or **Xon/Xoff** (software controlled) data flow control.

➤ NOTE

To avoid potential problems when communicating with the AP through the serial port, Proxim recommends that you leave the Flow Control setting at None (the default value).

Network Parameters

- **Serial Data Bits:** This is a read-only field and displays the number of data bits used in serial communication (8 data bits by default).
- **Serial Parity:** This is a read-only field and displays the number of parity bits used in serial communication (no parity bits by default).
- **Serial Stop Bits:** This is a read-only field that displays the number of stop bits used in serial communication (1 stop bit by default).

➤ NOTE

The serial port bit configuration is commonly referred to as **8N1**.

Network Time Protocol (NTP)

The Network Time Protocol (NTP) is a protocol that synchronizes computer clocks over the Internet. Devices that support NTP contact a known public time server to periodically retrieve the correct date and time. See <http://www.ntp.org/> for more information on this protocol.

By default, the AP boots up using January 1, 1970 as the date and 00:00:00 as the time. The AP does not necessarily need the correct date and time but you may want the AP to report the correct date and time if you intend to enable the [Logging](#) (Syslog) or [Credit Card Mirroring](#) functionality. Note that the AP's [System Status](#) alarms are reported in terms of the AP's **Up Time** and not in terms of standard date and time.

From the **NTP Server Configuration** screen, you can configure the AP-2500 to contact a network time server to retrieve the correct time and date each time the AP is turned on or rebooted. By default, NTP is disabled. If you want the AP to use the Network Time Protocol (NTP) to retrieve the time over the Internet, keep in mind the following:

- The AP will only contact a time server during boot-up. Therefore, you need to reboot the AP after configuring this.
- The AP must have a connection to the Internet to retrieve the date and time.
 - If the AP cannot communicate with a time server during boot-up, it will generate a major severity alarm, which is reported in the [System Status](#) screen as "No response from SNTP server." SNTP stands for Simple Network Time Protocol (a simplified version of the Network Time Protocol defined in RFC 2030 at <http://www.rfc-editor.org/>).
- See <http://www.ntp.org/> to identify the IP addresses for public time servers in your area.

You can also manually set the date and time from the NTP Server Configuration screen. However, if NTP is disabled, the AP will revert back to its default time (January 1, 1970 00:00:00) the next time it is rebooted (in other words, the AP does not store the date and time in non-volatile memory).

See [Configure the Date and Time](#) for step-by-step instructions for configuring the NTP parameters.

Filtering

The Access Point's Packet Filtering features help control the amount of traffic exchanged between the wired and wireless networks. There are two sub-categories under the Filtering heading.

- [Ethernet Protocol](#)
- [Static MAC](#)

Ethernet Protocol

The Ethernet Protocol Filter blocks or forwards packets based on the Ethernet protocols they support.

Follow these steps to configure the Ethernet Protocol Filter:

1. Configure the **Ethernet Protocol Filter Table**. This table is pre-populated with existing Ethernet Protocol Filters, however, you may enter additional filters by specifying the appropriate parameters.
 - To add an entry, click **Add**, and then specify the **Protocol Number** and a **Protocol Name**.
 - **Protocol Number:** Enter the protocol number. See <http://www.iana.org/assignments/ethernet-numbers> for a list of protocol numbers.
 - **Protocol Name:** Enter related information, typically the protocol name.

Network Parameters

- To edit or delete an entry, click **Edit** and change the information, or select **Enable**, **Disable**, or **Delete** from the **Status** drop-down menu.
 - An entry's status must be enabled in order for the protocol to be subject to the filter. The default filters are all disabled by default.
2. Select the interfaces or interfaces that will implement the filter from the **Ethernet Protocol Filtering** drop-down menu.
 - **Ethernet**: Packets are examined at the Ethernet interface
 - **Wireless A**: Packets are examined at the Slot A wireless interface
 - **Wireless B**: Packets are examined at the Slot B wireless interface
 - **All Interfaces**: Packets are examined at all interfaces
 - **Disabled**: The filter is not used
 3. Select the **Filter Operation Type**.
 - If set to **Passthru**, only the enabled Ethernet Protocols listed in the Filter Table will pass through the bridge.
 - If set to **Block**, the bridge will block enabled Ethernet Protocols listed in the Filter Table.
 4. Click **OK** to save your changes.
 5. Reboot the AP for your changes to take effect.

Static MAC

The Static MAC Address filter can prevent certain wireless clients from connecting to the network (based on the client's MAC address). For example, you can block all wireless clients from a single manufacturer from accessing your hotspot. This feature is similar to the [MAC Access](#) Table except you can use MAC address wildcards to block a range of addresses (for the MAC Access Table you specify a single MAC address).



NOTE

The Static MAC feature on the AP-2500 does not provide the same functionality as the Static MAC feature supported by the AP-2000 and AP-600. The AP-2500 supports the AP-2000/AP-600 Static MAC implementation only when the AP is operating in [Bridge mode](#).

Each static MAC entry contains the following fields:

- **Wired MAC Address**
- **Wired Mask**
- **Wireless MAC Address**
- **Wireless Mask**
- **Comment**: This field is optional.

Each MAC Address or Mask is comprised of 12 hexadecimal digits (0-9, A-F) that correspond to a 48-bit identifier. (Each hexadecimal digit represents 4 bits (each bit is a 0 or a 1).)

Follow these steps to configure the AP to block a range of MAC addresses from accessing the network:

1. Login to the AP's Web browser interface.
2. Click **Configure > Filtering > Static MAC**.
3. Click **Add**.
4. In the **Wired MAC Address** field, enter the MAC address or MAC address prefix that corresponds to the wireless devices that you want to block on the network.
 - Example: You want to prevent customers who purchased an unauthorized wireless card from accessing the network. The manufacturer of the unauthorized card uses a MAC address prefix of 00:03:8F (in other words, the MAC address of all of the cards from that manufacturer begin with 00:03:8F). Therefore, you would enter **00:03:8F:00:00:00** in the **Wired MAC Address** field.
5. In the **Wired Mask** field, enter a filter for the address you entered in the Wired MAC field. For best results, use *F*s or *0*s for each digit.
 - For the purposes of this feature, an *F* means that a device has to have the same digit as the Wired MAC Address for the filter to be applied.
 - For the purposes of this feature, a *0* means that a device does not need the same digit as the Wired MAC Address for the filter to be applied.

Network Parameters

- Examples:
 - If you set the Wired MAC Address to 00:03:8F:00:00:00 and you want to block all cards that begin with 00:03:8F, enter FF:FF:FF:00:00:00 as the Wired Mask. This will block any cards whose MAC address begins with those digits, ranging from 00:03:8F:00:00:00 to 00:03:8F:FF:FF:FF.
 - If you set the Wired MAC Address to a single MAC address (e.g., 00:03:8F:43:23:12), enter FF:FF:FF:FF:FF:FF as the Wired Mask. The filter will block only the specified address.
 - A Wired MAC Address of 00:03:8F:43:23:12 and a Wired Mask of FF:FF:FF:00:00:00 will also block any cards whose MAC address begins with 00:03:8F, ranging from 00:03:8F:00:00:00 to 00:03:8F:FF:FF:FF. To the filter, 00:03:8F:43:23:12 and 00:03:8F:00:00:00 are the same address; based on the specified Wired Mask, only the value of the first six digits matter.

⇒ NOTE

For the purposes of this filter, the *Wired Address* refers to a packet's source address. Therefore, all packets whose source address equals the Wired MAC Filter will be blocked by the AP.

6. Enter 00:00:00:00:00:00 in the **Wireless MAC** field.
7. Enter 00:00:00:00:00:00 in the **Wireless Mask** field.
8. Click **OK**.
9. Configure additional filters, if necessary.
10. Click the back arrow button to return to the previous screen.

An entry is enabled automatically after you click **OK**. To edit an entry, click **Edit**. To disable or remove an entry, click **Edit** and change the **Status** field from **Enable** to **Disable** or **Delete**.

The static MAC filter can be used to optimize the network performance by allowing filtering based on MAC addresses or groups of MAC addresses on wired and wireless interfaces. Groups of MAC addresses can be specified by using a bitmask.

For Example: If a block of MAC addresses (header consisting of 00-11-22) is to be filtered from wired to wireless interface, then the following can be configured:

Wired MAC Address: 001122AABBCC
 Wired Mask: FFFFFFFF000000 (This mask filters out all MAC addresses with a header of 00-11-22)
 Wireless MAC Address: 000000000000 (Enter all zeros since filtering wired MAC addresses)
 Wireless Mask: 000000000000 (Enter all zeros for the mask since filtering wired MAC addresses)

Wired MAC Address	Wired Mask	Wireless MAC Address	Wireless Mask	Comment	Status
00:03:8F:00:00:00	FF:FF:FF:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00		Enable

Figure 4-14 Static MAC Configuration Screen

Alarms

This category has two sub-categories.

- [Groups](#)
- [Alarm Host Table](#)

Groups

There are seven alarm groups that can be enabled or disabled:

- **Enable Configuration Alarms**
- **Enable Security Alarms**
- **Enable Wireless Alarms**
- **Enable Operational Alarms**
- **Enable Flash Memory Alarms**
- **Enable TFTP Alarms**
- **Enable Image Alarms**

Place a check mark in the box provided to enable a specific group. Remove the check mark from the box to disable the alarms.

These alarm groups correspond to System Alarms that are displayed in the Web browser interface's [System Status](#) screen and to traps that are sent by the AP to the SNMP managers specified in the [Alarm Host Table](#).

See [System Alarms \(Traps\)](#) for the list of alarms contained in each group.

Alarm Host Table

The Alarm Host Table contains the list of SNMP managers to which the AP will send SNMP trap messages. If the table is empty, the AP will not send SNMP traps onto the Ethernet network.

Follow these steps to add a Trap Host or SNMP manager to the Alarm Host Table:

1. Click **Configure > Alarms > Alarm Host Table**.
2. Click **Add**.
3. Enter the Trap Host's IP address in the **IP Address** field.
4. Enter the SNMP password (or community string) for the manager's trap group in the **Password** and **Confirm** fields.
5. Enter an optional comment, such as the alarm (trap) host station name.
6. Click **OK**.
7. Click the back arrow button to return to the previous screen.

To edit or delete an entry, click **Edit**. Edit the information, or select **Enable**, **Disable**, or **Delete** from the **Status** drop-down menu.

Network Parameters

Bridge

A traditional access point operates as a transparent bridge between your wired and wireless networking devices. The AP-2500 takes this a step further and provides Public Space features that facilitate hotspot operation (see [Public Space Features](#) and [Public Space Parameters](#) for details).

You can disable these Public Space features by enabling the AP's **Bridge Mode**. This mode effectively turns the AP-2500 into a traditional access point and simply forwards packets between its wired and wireless interfaces without any modification. You may find it useful to enable Bridge Mode for troubleshooting purposes if you or your subscribers are having difficulty communicating with the Internet.

Follow these steps to enable Bridge Mode:

1. Click **Configure** > **Bridge**.
2. Place a check mark in the **Enable Bridge Mode** box.
3. Click **OK**.
4. Reboot the AP for your change to take effect.



CAUTION

Bridge Mode is provided for troubleshooting purposes only. All of the AP's Public Space features are disabled when Bridge Mode is enabled.

To disable Bridge Mode, remove the check mark from the **Enable Bridge Mode** box, click **OK**, and reboot the AP.

Security

The AP-2500 offers several security features to protect your network from unauthorized individuals. You also configure the RADIUS settings within the Security configuration screens.

- [MAC Access](#)
- [RADIUS](#)
- [Encryption](#)
- [VPN](#)

MAC Access

The **MAC Access** tab allows you to build a list of wireless clients authorized to access the network through the AP. The wireless clients are identified by their unique MAC addresses.

For example, if a thief steals one of your authorized subscriber cards, you can enter the missing card's MAC address in the MAC Access Control Table and set the Operation Type to Block. In this case, the thief will be unable to access the Internet through the AP-2500 using the stolen card.

Note that you must reboot the AP for any changes to the MAC Access Control Table to take effect.

Follow these steps to configure the MAC Access Control Table:

1. Click **Configure** > **Security** > **MAC Access**.
2. Click **Add**.
3. Enter the MAC address of the wireless card that you want to add to the table in the **MAC Address** field.
 - Enter the MAC address as 12 digits without space (for example, 000222D738462) or separate each pair of digits with colons (for example, 00:02:2D:73:84:62).
 - A wireless card's MAC address is typically found on the label on the back of the card.
4. Enter an optional **Comment** in the field provided.
5. Click **OK**.
6. Repeat this procedure to add the MAC address of any other card you want to include in the table.
7. Click the back arrow button to return to the previous screen.
8. Place a check mark in the **Enable MAC Access Control** box.

Network Parameters

9. Select an **Operation Type** from the drop-down menu. This determines how the stations identified in the MAC Access Control Table are filtered.
 - If set to **Passthru**, only the addresses listed in the Control Table will pass through the AP.
 - If set to **Block**, the AP will block traffic to or from the addresses listed in the Control Table.
10. Click **OK** to save your changes.
11. Reboot the AP for your changes to take effect.

To edit or delete an entry, click **Edit**. Edit the information, or select **Enable**, **Disable**, or **Delete** from the **Status** drop-down menu.

System **Network** **Interfaces** **Management**

Filtering **Alarms** **Bridge** **Security**

MAC Access **RADIUS** **Encryption** **VPN**

This feature can be used to deny or allow network access to wireless clients associated to the access point. The MAC access control table is used to enter the wireless client's MAC Addresses.

Note: Changes to these parameters require access point reboot in order to take effect.

Enable MAC Access control ☒

Operation Type **Block**

OK **Cancel**

MAC Access Control Table

Add **Edit**

MAC Address	Comment	Status
00:02:2D:73:84:62		Enable
00:20:A6:12:34:56		Enable

Figure 4-15 MAC Access Configuration Screen

Subscribers and MAC Access Control

MAC Access Control does not prevent wireless clients from associating with an Access Point but it does prevent unauthorized clients from communicating with the Access Point. For example, the client software on a blocked wireless subscriber will report that the card is linked to the AP but the AP (acting as a DHCP server) will not assign the client an IP address.

Validation within the MAC Access Control Table occurs before a client is authenticated by the AP-2500 using internal or external authentication (see [AP-2500 Authentication Methods](#) for an explanation of these options). For example, a subscriber whose card is blocked by the MAC Access Control Table will never be given the opportunity to logon to the Internet even if he has a valid User Name and Password.

Network Parameters

RADIUS

- [RADIUS Overview](#)
- [Unique AP-2500 RADIUS Client Features](#)
- [RADIUS Messages and RADIUS Attributes](#)
- [Sample RADIUS Transmissions](#)
- [RADIUS Configuration Parameters](#)

RADIUS Overview

RADIUS is a proven carrier-class protocol to perform accurate time and volume-based billing. The RADIUS protocols are defined in RFCs 2865 (Authentication) and 2866 (Accounting). These RFCs are available at <http://www.rfc-editor.org/>. Coming from the traditional dial-up Internet access world, this mature protocol has been adapted to perform the same tasks in modern broadband environments, both for public access and residential solutions. The core RADIUS client implementation of the AP-2500 is being used in carrier networks every day by hundreds of thousands of users worldwide, providing accurate authentication and accounting information in conjunction with virtually all major RADIUS servers (e.g. Lucent, Funk, and Cisco).

The AP's RADIUS client implementation is characterized not only by carrier-class redundancy, but also by an innovative implementation of new features improving:

- Authentication security (e.g. SSL)
- Authentication accuracy (e.g. MAC address transmission)
- Accounting accuracy (e.g. accurate time stamps and bytes sent/received information even during network maintenance)
- Accounting flexibility (interim accounting messages)
- User convenience to maximize revenues (e.g. ability to dynamically change service plan and update accounting records in real time)

Unique AP-2500 RADIUS Client Features

The AP-2500 provides a number of unique RADIUS-driven features that improve the customer experience.

Dynamic Service Plan Change via ICC

The AP allows the end-user to dynamically change his service plan without contacting a system administrator. The billing records are kept up-to-date via a real-time RADIUS accounting request message. This feature lets you upsell a premium service plan to premium users with no additional costs. For example, a user may be synchronizing his email at an airport when he finds that a co-worker has sent him a 20 Mbyte presentation. Since the user only subscribes to the most cost effective plan at 256 Kbits/sec, it may mean that he has to miss his plane because he cannot exceed this speed. With the AP-2500, the user can simply choose a faster plan and only get billed for the time he is using the plan.

The ICC JAVA applet also contains a **Logout** button that allows the end-user to terminate a session (explicit logout). Upon pressing the Logout button and confirming the explicit session termination request in an additional pop-up window, the ICC will send an XML command to the AP. The AP then immediately sends an Accounting Stop message to the RADIUS server. Alternatively, the user can also type <http://1.1.1.1/> into his browser to initiate a session termination. An appropriate confirmation message will be shown in the user's browser to confirm the explicit session termination. See [Information and Control Console \(ICC\)](#) for more information on the ICC.

Automatic Re-transmission and "Remember Me" Cookie

Most network operators consider it important to implement short idle time-outs to improve network efficiency. Idle-time-outs can be effectively used to ensure accurate billing for users that either turn off their laptop or lose network access for any other reason (such as the AP becomes inoperable). Therefore, the user will have to login again after a period of inactivity. However, the AP supports two features to improve the user experience: RADIUS re-authentication and the "Remember Me" cookie. Both features allow the user to seamlessly re-authenticate upon entering the network again without having to type in the user name and password. See [Enabling Cookie Support](#) for more information on the "Remember Me" option.

Network Parameters

Data Volume Information Transmission (bytes sent/received)

The AP's RADIUS client implementation allows a hotspot operator to accurately track the exact number of bytes sent and received by a subscriber based on:

- User Name
- IP address (Framed IP)
- MAC address of the user (Calling Station ID)

As shown in the [Sample RADIUS Transmissions](#), the byte counts are sent in the Accounting "Alive" and Accounting "Stop" messages. As mentioned previously, Accounting "Stop" messages can be generated by:

- An explicit customer logout (via ICC or by typing <http://1.1.1.1/>)
- Session time-out
- Idle time-out
- Deleting the user from the AP's [Current Subscribers Table](#).

The message will indicate the type of action that initiated the Accounting "Stop". To ensure accuracy, the AP temporarily saves the Accounting information per user in case of a device reboot.

RADIUS Messages and RADIUS Attributes

The AP-2500's RADIUS functionality can be broken down into the following categories:

- **Access-Request**
- **Access-Accept Parsing**
- **Acct-Request**

Access-Request Attributes

- Username
 - Included if enabled.
- Password
- Service-Type
- NAS-Port (communication port number)
- NAS-Identifier
 - Included if enabled on AP; see [RADIUS Configuration Parameters > Miscellaneous Options](#).
- Framed-IP
 - The subscriber's IP address.
 - Included if enabled on AP; see [RADIUS Configuration Parameters > Miscellaneous Options](#).
- Called-Station-Id
 - The AP's MAC address.
- Calling-Station-Id
 - The subscriber's MAC address.
- NAS-IP
 - The AP's IP address
- NAS-Port-Type
 - Included if enabled on AP; see [RADIUS Configuration Parameters > Miscellaneous Options](#).
- Acct-Session-ID
 - The Acct-Session-ID is created when the RADIUS authentication request is built. It is transmitted in both the Access-Request and the Accounting-Request.
- State
 - Used for challenge/response authentication; since the AP uses the Password Authentication Protocol (PAP) for authentication purposes, this attribute is not currently in use.

Access-Accept Parsing

- Reply-Message
 - Used for challenge/response authentication; since the AP uses the Password Authentication Protocol (PAP) for authentication purposes, this attribute is not currently in use.
- State
 - Used for challenge/response authentication; since the AP uses the Password Authentication Protocol (PAP) for authentication purposes, this attribute is not currently in use.
- Class
 - This is a customizable attribute for accounting purposes. If defined at your RADIUS server, the AP will pass this attribute to the Accounting server (if Accounting is enabled).
- Session-Timeout
 - If the RADIUS server does not send a Session-Timeout, the AP will set the subscriber expiration time to 0, which means indefinite access.
 - There is a two-minute margin of error for this parameter. In other words, it can take between 1 and 120 seconds for the AP to send an accounting “stop” message after the Session-Timeout has expired.
- Idle-Timeout
 - You can set a default time-out from the AP’s **Network > Security > RADIUS** screen. If the Radius server does not send an Idle-Timeout in the RADIUS Access-Accept message, the AP will use the default one to disconnect subscribers. The AP also uses the default timer if the Idle-Timeout attribute specifies a time period greater than the default timeout.
 - There is a two-minute margin of error for this parameter. In other words, it can take between 1 and 120 seconds for the AP to send an accounting “stop” message after the Session-Timeout has expired.
- Acct-Interim-Interval
 - Specifies the frequency with which the AP sends a RADIUS Accounting Interim message for the specific subscriber. If this attribute is not present or equal to 0, no Interim message is sent. Note that the AP will not send Interim messages more frequently than every 2 minutes.
- *Nomadix Vendor Specific Attributes*

The AP-2500 supports the following Vendor Specific Attributes from Nomadix, Inc.:

 - **Nomadix-Bw-Up** (integer)
 - This attribute value (in Kbps) restricts the speed at which subscriber uploads are performed.
 - **Nomadix-Bw-Down** (integer)
 - This attribute value (in Kbps) restricts the speed at which subscriber downloads are performed.
 - **Nomadix-URL-Redirection** (string)
 - This attribute allows the administrator to redirect the user to a page of the administrator's choice after every successful login.
 - This redirect command takes precedence over the [Home Page Redirection \(HPR\)](#) option.
 - You need to enable the **URL Redirection** option in the **Configure > Network > Security > RADIUS** screen if you want to use this attribute.
 - **Nomadix-IP-Upsell** (integer)
 - This attribute allows the user to receive a public address from a DHCP pool (managed by the Relay DHCP server) when the AP has the IP-Upsell feature enabled.

Network Parameters

Acct-Request

- Username
- Called-Station-Id
- Calling-Station-Id
- Acct-Status-Type (Start/Stop/Alive)
- Acct-Session-ID
- Acct-Output-Octets
 - Number of octets (bytes) sent by subscriber.
- Acct-Input-Octets
 - Number of octets (bytes) received by subscriber.
- Acct-Output-Packets
 - Number of packets sent by subscriber.
- Acct-Input-Packets
 - Number of packets received by subscriber.
- Class
- Acct-Session-Time (Stop)
 - Acct-Session-Time is calculated the following way (for each transmitted/retransmitted Acct-Stop):
Acct-Session-Time = time of last sent packet - subscriber login time.
- Acct-Terminate-Cause (Stop)
 - 1 = User Requested; 4 = Idle Timeout; 5 = Session Timeout
- NAS-IP
- NAS-Port-Type
- NAS-Port
- Framed-IP
- Acct-Delay-Time
- *Nomadix Vendor Specific Attributes*
The AP-2500 supports the following Vendor Specific Attributes from Nomadix, Inc.:
 - Nomadix-Bw-Up (integer)
 - Nomadix-Bw-Down (integer)
 - Nomadix-URL-Redirection (string)
 - Nomadix-IP-Upsell (integer)

The AP-2500 will also wait for the receipt of an Accounting Reply message. If no reply is received, the AP will retransmit the message based on the configuration of the [Retransmission Options](#).

Notes:

- **NAS** stands for Network Access Server. This refers to the AP-2500.
- Vendor Specific Attributes are also referred to as **VSAs**.

Network Parameters

Sample RADIUS Transmissions

These are actual accounting logs from a Lucent Navis RADIUS server with all VSAs enabled.

Accounting Start Message

Thu Aug 29 12:45:32 2002
User-Name = "testflo"
NAS-IP-Address = 64.209.75.102
NAS-Port = 0
Acct-Status-Type = Start
Acct-Session-Id = "98000004"
Called-Station-Id = "00-20-A6-00-12-3E"
Calling-Station-Id = "00-04-AC-25-EB-2D"
NAS-Identifier = "Location ABC"
NAS-Port-Type = 19
Framed-IP-Address = 56.57.58.59
Nomadix-IP-Upsell = 0
Acct-Delay-Time = 0

Accounting Interim Message

Thu Aug 29 12:48:54 2002
User-Name = "testflo"
NAS-IP-Address = 64.209.75.102
NAS-Port = 0
Acct-Status-Type = Alive
Acct-Session-Id = "98000004"
Acct-Output-Octets = 10200
Acct-Input-Octets = 276874
Acct-Output-Packets = 93
Acct-Input-Packets = 393
Nomadix-Bw-Up = 256
Nomadix-Bw-Down = 256
Called-Station-Id = "00-20-A6-00-12-3E"
Calling-Station-Id = "00-04-AC-25-EB-2D"
Acct-Session-Time = 202
NAS-Identifier = "Location ABC"
NAS-Port-Type = 19
Framed-IP-Address = 56.57.58.59
Nomadix-URL-Redirection = "http://www.msn.com/"
Nomadix-IP-Upsell = 1
Acct-Delay-Time = 0

Network Parameters

Accounting Alive Message Caused by Explicit Service Plan Change

Thu Aug 29 12:49:20 2002
User-Name = "testflo"
NAS-IP-Address = 64.209.75.102
NAS-Port = 0
Acct-Status-Type = Alive
Acct-Session-Id = "98000004"
Acct-Output-Octets = 36440
Acct-Input-Octets = 512195
Acct-Output-Packets = 284
Acct-Input-Packets = 630
Nomadix-Bw-Up = 56
Nomadix-Bw-Down = 56
Called-Station-Id = "00-20-A6-00-12-3E"
Calling-Station-Id = "00-04-AC-25-EB-2D"
Acct-Session-Time = 228
NAS-Identifier = "Location ABC"
NAS-Port-Type = 19
Framed-IP-Address = 56.57.58.59
Nomadix-URL-Redirection = "http://www.msn.com/"
Nomadix-IP-Upsell = 1
Acct-Delay-Time = 0

Accounting Stop Message

Thu Aug 29 12:49:45 2002
User-Name = "testflo"
NAS-IP-Address = 64.209.75.102
NAS-Port = 0
Acct-Status-Type = Stop
Acct-Session-Id = "98000004"
Acct-Output-Octets = 40644
Acct-Input-Octets = 525734
Acct-Output-Packets = 316
Acct-Input-Packets = 679
Nomadix-Bw-Up = 56
Nomadix-Bw-Down = 56
Called-Station-Id = "00-20-A6-00-12-3E"
Calling-Station-Id = "00-04-AC-25-EB-2D"
Acct-Session-Time = 248
Acct-Terminate-Cause = Session-Timeout
NAS-Identifier = "Location ABC"
NAS-Port-Type = 19
Framed-IP-Address = 56.57.58.59
Nomadix-URL-Redirection = "http://www.msn.com/"
Nomadix-IP-Upsell = 1
Acct-Delay-Time = 0

Network Parameters

RADIUS Configuration Parameters

You can configure the AP to communicate with up to four different RADIUS servers:

- Primary Authentication Server
- Back-up Authentication Server
- Primary Accounting Server
- Back-up Accounting Server

➤ NOTE

You must configure the settings for at least one Authentication server before configuring the settings for an Accounting server.

The back-up servers are optional, but when configured, the AP will communicate with the back-up server if the primary server is off-line. You can configure the same server to perform both Authentication and Accounting services.

You can configure the following parameters from the AP's **Configure > Network > Security > RADIUS** screen. If you are using RADIUS with Internal Authentication, see [Internal Authentication with RADIUS](#) for additional information and step-by-step configuration instructions.

The RADIUS access control provides authentication of wireless clients via a standard RADIUS server(s). Primary and backup RADIUS servers can be configured.

Note: In order to enable the RADIUS authentication feature, at least one RADIUS server must be configured.

Note: Changes to these parameters require access point reboot in order to take effect.

RADIUS Servers	Authentication	Accounting
Enable Servers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Primary Server IP Address	204.23.12.51	204.23.12.52
Primary Server DNS Name		
Primary Server Port	1812	1813
Primary Server Secret Key	*****	*****
Secondary Server IP Address	0.0.0.0	0.0.0.0
Secondary Server DNS Name		
Secondary Server Port	0	0

Figure 4-16 RADIUS Configuration Screen

RADIUS Servers

- **Enable Servers:** Place a check mark in the appropriate box to enable the AP's RADIUS client for Authentication and/or Accounting.

➤ NOTE

The Server settings below apply to both the Primary RADIUS server and the optional Secondary RADIUS server.

Network Parameters

- **Server IP Address:** The IP address of the RADIUS server (separate fields for Authentication and Accounting).
- **Server DNS Name:** The DNS Name of the RADIUS server (separate fields for Authentication and Accounting).

⇒ NOTE

Enter either the Server IP Address or the Server DNS Name, but not both.

- **Server Port:** The port on which the RADIUS server operates.
 - This port must match the RADIUS Authentication or Accounting port supported by your RADIUS program.
 - Most RADIUS servers use port 1812 (the default setting) for Authentication and port 1813 (the default setting) for Accounting. However, Funk Steel-belted RADIUS uses port 1645 for Authentication and 1646 for Accounting.
- **Server Secret Key:** This is a password between the AP and the RADIUS server. Enter the same Shared Secret that you used when you added the AP as a client on the RADIUS server.

Retransmission Options

- **Retransmission Method:** Set to **Failover** or **Round-Robin**. This option is only valid if you have configured settings for a Secondary Server.
 - **Failover:** The AP make multiple attempts to reach the Primary Server. If the Primary Server fails to respond (after the specified number of Retransmission Attempts), the AP falls over to the Secondary Server.
 - **Round-Robin:** The AP first attempts to reach the Primary Server. If the Primary Server fails to respond, the AP tries the Secondary Server. If the Secondary Server fails to respond, the AP again tries the Primary Server.
- **Retransmission Frequency:** The number of seconds between retransmission attempts. Default is 3 seconds.
- **Retransmission Attempts:** The number of retransmission attempts (per server). Default is 2 (per server).
- **Retransmission Timeouts:** The number of seconds after which a retransmission attempt times out.

ISP Account Creation

⇒ NOTE

This option is provided for demo purposes. It acts as a portal page HTTP redirection to allow new users to sign up for service with an ISP.

- **Enable ISP Account Creation:** Place a check mark in this box to enable this feature.
- **ISP Portal Page URL:** Specifies a Web site to which subscribers are redirected after submitting an HTTP request (prior to authentication).
- **ISP Account Creation URL:** Specifies a Web site on the ISP's server that contains an account creation form for new subscribers.
- **ISP Server IP:** The IP address of the ISP's server that hosts the portal and account creation pages.

⇒ NOTE

If you enable this feature for demo purposes, you must also add the ISP Server's IP address to the Passthrough IP Table.

Miscellaneous Options

- **User Name/Password Type:** Determines what credentials the RADIUS server uses to authenticate subscribers.
 - **User-Input** (that is, User Name and Password)
 - **MAC-MAC** (The wireless card's MAC address is used as both the user name and the password)
 - **MAC-Key** (The wireless card's MAC address is the user name and the AP/RADIUS **Shared Secret** is the password)
 - If using **MAC-MAC** or **MAC-Key**, enter the MAC address in the following format: 123456-7890ab (6 digits, a dash, final 6 digits).

Network Parameters

- **Enable RADIUS Profile Caching:** When enabled, the AP maintains the user's information in the [Current Subscribers Table](#) (**State: Pending**) after a user logs out or times out. If the user attempts to re-connect, he can access the service again without being prompted to re-enter his user name and password.

➤ NOTE

This option uses the subscriber card's MAC address to re-validate the user. For security reasons, you may not want to enable this option. It is theoretically possible that an unauthorized individual could capture the user's MAC address and use it to spoof the AP to connect to the network when the actual user is not logged in.

- **Enable URL Redirection:** When enabled, the AP uses the configured Nomadix-URL-Redirection VSA to redirect an authenticated subscriber to the Web site specified by the VSA. Note that this option takes precedence over the [Home Page Redirection \(HPR\)](#) option (that is, if you have HPR enabled and you have configured the Nomadix-URL-Redirection VSA, a RADIUS client will be redirected to the page specified by the VSA and not by HPR).
- **Send Framed IP:** When enabled, the IP address assigned to the client is included in the messages sent to RADIUS server.
 - You can use this parameter to help identify the IP address assigned to clients in the RADIUS accounting logs. If using IP Upsell, you can also see how many clients are using public IP addresses.
- **Send NAS Identifier:** When enabled, the AP's NAS Identifier is included in the messages sent to the RADIUS server.
- **NAS Identifier:** Specifies a unique identifier for the AP that is included within RADIUS messages if you enabled **Send NAS Identifier**. (In RADIUS terminology, the AP is the NAS or Network Access Server.)
 - You can use this parameter to differentiate between multiple APs in the RADIUS accounting logs.
 - Also, the RADIUS server can alter a user's access policy depending on the NAS identifier. For example, the maximum session time could be reduced if the NAS identifier is "restaurant" instead of "library."
- **Send NAS Port Type:** When enabled, the NAS port type is included in the messages sent to the RADIUS server.
- **NAS Port Type:** The port number that is included within RADIUS messages if you enabled **Send NAS Port Type**. Set this to **19** if you want to use this parameter.
 - Port Type 19 corresponds to a connection made over an IEEE 802.11 Wireless network. See RFC 2865 for details (the RFC is available at <http://www.rfc-editor.org/>).
 - You can also use NAS Port Type to establish different access policies. For example, in a cyber café there could be two access types: wired and wireless and you could charge more for access from a wired computer that is part of your network infrastructure.
- **Default User Idle Timeout:** The AP times out users who are inactive for the specified number of seconds.
 - The AP only uses this parameter if the Idle-Timeout attribute is not set or if the attribute specifies an amount of time that is greater than this setting. See [RADIUS Messages and RADIUS Attributes](#) for details.
 - When set to 0, a user never times out (assuming that the Idle-Timeout attribute is not set).

Network Parameters

Encryption

The IEEE 802.11 standards specify an optional encryption feature, known as Wired Equivalent Privacy or WEP, that is designed to provide a wireless LAN with a security level equal to what is found on a wired Ethernet network. WEP encrypts the data portion of each packet exchanged on an 802.11 network using an Encryption Key (also known as a WEP Key).

When Encryption is enabled, two 802.11 devices must have the same Encryption Keys and both devices must be configured to use Encryption in order to communicate. If one device is configured to use Encryption but a second device is not, then the two devices will not communicate, even if both devices have the same Encryption Keys.

- The AP-2500 supports 64-bit and 128-bit encryption (for both 802.11a and 802.11b).
 - For 64-bit encryption, an encryption key is 10 hexadecimal characters (0-9 and A-F) or 5 ASCII characters (see [ASCII Character Chart](#)).
 - For 128-bit encryption, an encryption key is 26 hexadecimal characters or 13 ASCII characters. Note that some 802.11b cards do not support 128-bit encryption.



NOTE

64-bit encryption is sometimes referred to as 40-bit encryption; 128-bit encryption is sometimes referred to as 104-bit encryption.

Keep in mind that if you enable WEP encryption on the wireless interfaces, you will need to inform your subscribers of these settings and they will need to reconfigure their wireless cards with these settings before gaining access to the network (and before they are prompted to logon to the hotspot).

See [Set WEP Encryption for each Wireless Interface](#) for step-by-step configuration instructions.

VPN

Many companies support Virtual Private Network (VPN) connections to provide secure network access for employees in remote locations. The VPN connection establishes a secure, encrypted tunnel between the employee and the company's VPN server over the public Internet.

VPNs are a popular application for hotspot subscribers. For example, a business traveler can establish a VPN session with his company's network at an airport or a hotel and access the same network resources that are available to him when he's physically in the office.

To create a VPN connection, a company needs a VPN server on the Internet. An employee needs VPN client software installed on his computer and a connection to the Internet. There are multiple tunneling and encapsulation techniques available and can vary from company to company.

In general, a subscriber with a public, routable IP address can establish a VPN session with his company without involving the AP-2500. However, most subscribers in your hotspot will use private IP address assigned by the AP performing Network Address Translation (NAT). (See [Dynamic Address Translation \(DAT\)](#) for information on NAT.) Therefore, you must configure the AP to support VPN connections.

The AP-2500 supports two of the most popular VPN protocols when performing NAT:

- Point-to-Point Tunneling Protocol (PPTP)
- Internet Protocol Security Protocol (IPSec) using Encapsulating Security Payload (ESP)

The VPN configuration information is found at **Configure > Network > VPN**. By default, these two protocols are enabled. Follow these steps if you want to change the default VPN settings:

1. Click **Configure > Network > VPN**.
2. Configure the **Enable PPTP** field to enable or disable PPTP support.
 - By default, PPTP is enabled.
3. Enter the number of seconds after which an idle PPTP connection will time-out in the **PPTP Idle Timeout** field.
 - By default, this is set to 0 seconds; this means that an idle connection will never time-out.
4. Configure the **IPSec** field to enable or disable IPSec support.
 - By default, IPSec is enabled.
5. Click **OK**.
6. Reboot the AP for your changes to take effect.

Special Considerations Regarding VPN Support

The most common VPN protocol is IPSec. When a subscriber who has a private IP address (assigned via NAT) attempts to create a VPN session, the AP-2500 performs a mapping between the subscriber's private IP address and the AP's public IP address. This is also known as **IPSec Traversal**.

However, your subscribers may encounter a problem establishing VPN sessions when using private IP addresses. Potential causes include:

- **Customer uses an IPSec mode other than ESP:** The AP-2500 supports only Encapsulating Security Payload (ESP) tunnel mode. This is the most common mode of establishing IPSec tunnels. In the rare case that a subscriber is using one of the other methods, then it would be necessary for this user to be given a public IP address. Other IPSec methods are Authentication Header (AH) transport and tunnel mode and ESP transport mode.
- **Two or more subscribers attempt to connect to the same VPN server:** In general, most VPN servers support only a single IPSec session from a particular public IP address. However, when establishing a VPN session, all subscribers connected to a particular AP will share the same originating IP address (that is, the AP's public IP address). When a VPN server sees multiple session requests from the same IP address it typically drops all connections which originate from that address. Note that this is not a problem with the AP's NAT functionality; it is an issue with the VPN server that will not support multiple connections from the same IP address. This behavior does not apply to all VPN servers. At the release of this documentation, VPN servers from Cisco and Lucent do not support more than one IPSec session from the same IP address but the VPN server from Nortel Networks does support multiple sessions.

These problems should be addressed in the future as new VPN techniques are introduced. Recently, a method has been developed and implemented by some VPN server manufacturers to use a UDP header to encapsulate the IPSec packet. This technique allows multiple IPSec sessions to originate behind a NAT device and does not require the NAT device to be aware of these IPSec sessions. (This method applies to both ESP tunneled mode and ESP transport mode but not to either AH mode.) As the AP-2500 would be unaware of these IPSec sessions, it would not be necessary to provide customers with public IP addresses.

However, until these methods become widely deployed, you will need to notify your hotspot subscribers of these potential connectivity problems. If you have a pool of public IP address, you can use the [IP Upsell](#) feature to supply public IP addresses (for a fee) to those customers who experience the problems outlined above. But, even if you do not plan to offer public IP addresses, you should still inform your customers of these VPN limitations (for example, you could have a link to a VPN statement on your Portal Page).

5

Public Space Parameters

In this Chapter

This chapter describes all of the Public Space operating parameters that can be configured using the Access Point's Web browser interface (that is, the parameters accessible after clicking the **PublicSpace** or **Subscriber** button).

⇒ NOTE

If this is your first time configuring the AP-2500, be sure to read [AP-2500 Authentication Methods](#) for information on the available AAA techniques and for step-by-step configuration instructions.

PublicSpace Options

- [Home Page Redirection \(HPR\)](#): Configures the Home Page Redirection feature, which sends subscribers to a specified page following successful authentication.
- [Authentication, Authorization, and Accounting \(AAA\)](#): These settings configure the AP's Authentication mode.
 - [AAA Basic](#)
 - [AAA Services with an External Web Server \(EWS\)](#)
 - [AAA Services with the Internal Web Server \(IWS\)](#)
- [Logging](#): Configures the AP to send system and AAA messages to a Syslog server.
- [URL Filtering](#): Blocks subscriber access to a list of specified Web sites.
 - [URL Filtering by DNS Names](#)
 - [URL Filtering by IP Address](#)
- [Information and Control Console \(ICC\)](#): Configures the Java pop-up window that appears on subscriber's Web browser screens.
- [SMTP Redirection](#): Enables redirection of outgoing e-mails to a specified SMTP server.
- [Passthrough Addresses](#): Configures the list of DNS Names and/or IP addresses that can be accessed by unauthorized users to create a "walled garden".
 - [Passthrough DNS Table](#)
 - [Passthrough IP Table](#)
 - [Passthrough AAA Port](#)
- [Bandwidth Management](#): Notifies the AP of the maximum bandwidth speeds available to it so the AP can effectively manage subscriber bandwidth.

Subscriber Options

- [Billing Options for Subscribers](#): Configures the billing options available to subscribers if using internal authentication.
- [Subscriber Messages](#): Configures messages that appear on the AP's IWS pages.
- [Authorized Subscribers](#): The table containing the list of subscribers authorized via internal authentication.

⇒ NOTE

See [Logging into the Web Interface](#) for instructions on how to access the AP's Web browser interface.

Home Page Redirection (HPR)

This tab is used to redirect the subscriber's browser to a specified home page following successful authentication. To redirect subscribers to a specified page before authentication, use the Portal Page feature with internal authentication (see [Portal Page](#)) or use external authentication (see [External Authentication](#)).

Note that the Nomadix-URL-Redirection RADIUS Vendor Specific Attribute (VSA) takes precedence over the Home Page Redirection option (that is, if you have HPR enabled and you have configured the Nomadix-URL-Redirection VSA, a RADIUS client will be redirected to the page specified by the VSA and not by HPR). See [RADIUS Messages and RADIUS Attributes](#).

Follow these steps to enable Home Page Redirection:

1. Login to the Web browser.
2. Click **PublicSpace > HPR**.
3. Place a check mark in the **Enable Home Page Redirection** box.
 - If Home Page Redirection is disabled and you do not use a Portal Page, the subscriber will be redirected to the Web site that he/she initially requested prior to authentication.
4. Place a check mark in the **Enable Parameter Passing** box, if applicable.
 - This parameter is optional. You do not need to enable this parameter if you want to direct customers directly to a particular site (such as <http://www.myhotspot.com>) after successful authentication. You should enable this optional only if you want to return the subscriber to the Web site that he/she requested prior to authentication (and you use a Portal Page).
 - If you use a Portal Page, the AP-2500 can track a subscriber's initial Web request (typically the subscriber's home page) when Parameter Passing is enabled. Then, after successful authentication, you can direct the subscriber back to this page from a customized confirmation screen (see the *confirm.asp* sample described in the [Portal Page](#) section for an example of this).
 - The sample ASP portal pages contain an example of how to store and retrieve the subscriber's initial Web request (known as the Originating Server or OS). See [Portal Page](#) for more information.



NOTE

When Parameter Passing is enabled, the AP-2500 converts an OS statement in DNS format to an IP address. If a customer's OS request is for a URL that contains subdirectories (such as <http://www.myhotspot.com/mysite/index.html>), then the AP may truncate this to the site's default Web page (<http://www.myhotspot.com/>) following the DNS to IP conversion. Therefore, after successful authentication, a user may not necessarily be redirected to the site he/she initially requested.

5. Enter the address for the page to which authenticated subscribers will be directed in the **Redirected URL** field.
 - You must configure DNS if you want to enter meaningful URLs instead of numeric IP addresses.
6. Enter a **Redirection Frequency** in the field provided. This is the number of minutes that will elapse before a subscriber is automatically redirected back to the specified **Redirection URL**.
 - By default, this parameter is set to 3600 minutes (60 hours).
 - Do not set this parameter to 0; your subscribers will be redirected to the specified Redirection URL each time he/she tries to access a new Web page.
7. Click **OK**.

Public Space Parameters

The screenshot shows the 'PublicSpace' configuration window with the 'HPR' tab selected. The window has a sidebar with buttons: Status, Configure, Monitor, Commands, PublicSpace (highlighted), Subscriber, Help, and Exit. The main content area has tabs for ICC, SMTP, Passthrough, Bandwidth Mgmt, HPR (selected), AAA, Logging, and URLFilter. The HPR tab contains the following text: 'This tab is used to configure Home Page Redirection (HPR). HPR, if enabled, redirects subscribers browser to the specified URL.' and a note: 'Note: DNS must be properly configured to enter URLs instead of numeric IP addresses. If HPR is enabled, URL for the redirected home page must be entered.' Below this is the 'Home Page Redirection Configuration' section with the following fields: 'Enable Home Page Redirection' (checkbox, unchecked), 'Enable Parameter Passing' (checkbox, unchecked), 'Redirection URL' (text box containing 'http://www.cnn.com'), and 'Redirection Frequency' (text box containing '15' with 'Mins' next to it). At the bottom are 'OK' and 'Cancel' buttons.

Figure 5-1 Home Page Redirection Configuration

Authentication, Authorization, and Accounting (AAA)

The AP-2500 uses AAA services to authenticate, authorize, and subsequently bill subscribers for their use of the customer's network. This section describes the parameters that can be configured from the **AAA** tab. See [AP-2500 Authentication Methods](#) for detailed information on the available authentication methods.

AAA Basic

This tab provides information needed to set up AAA basic settings that apply to all authentication methods.

The screenshot shows the 'AAA' configuration window with the 'Basic' tab selected. The window has the same sidebar as Figure 5-1. The main content area has tabs for ICC, SMTP, Passthrough, Bandwidth Mgmt, HPR, AAA (selected), Logging, and URLFilter. The AAA tab contains the following text: 'This tab is used to configure the basic settings for Authentication, Authorization and Accounting (AAA) service.' and a note: 'Note: If XML Interface is enabled, XML Sender IP address field must be entered.' Below this is the 'Basic' configuration section with the following fields: 'Enable AAA Services' (checkbox, unchecked), 'Enable XML Interface' (checkbox, checked), 'XML Sender IP Address' (text box containing '255.255.255.255'), and 'Authorization Method' (radio buttons, 'Internal' selected). At the bottom are 'OK' and 'Cancel' buttons.

Figure 5-2 AAA Basic Screen

Public Space Parameters

- **Enable AAA Services:** Enable this option to support any of the authentication methods described in [AP-2500 Authentication Methods](#). When disabled, wireless users will have access to the Internet without authentication; this is the default setting.
- **Enable XML Interface:** Enable this option to configure the AP to support XML (Extensible Markup Language) commands received from the XML Sender IP Address. The XML interface can be used with Internal or External authentication but is generally used in conjunction with External authentication. XML commands are appended to a URL in the form of an encoded query string. The AP parses the query string, executes the commands specified by the string, and returns data to the IP address that initiated the command request. See [XML Interface Specification](#) for details.
- **XML Sender IP Address:** The IP address of the external device that can send XML commands to the AP. If using EWS authentication, this should be the IP address of your External Web Server. If using IWS authentication, enter the IP address of the network computer from which the AP will accept XML commands (XML is optional with IWS authentication).
- **Authentication Method:** After enabling AAA Services, select your authentication method: **Internal** Web Server (IWS) or **External** Web Server (EWS).

AAA Services with an External Web Server (EWS)

You set the configuration parameters for your External Web Server (EWS) from the **PublicSpace > AAA > External** screen. When AAA services are enabled with an EWS (when **PublicSpace > AAA > Basic > Authentication Method** is set to **External**), the AP-2500 redirects the subscriber's login request to an external server. The login page served by the EWS reflects the "look and feel" of the solution provider's network and presents more login options.



NOTE

See [External Authentication](#) for information on the external authentication process and for step-by-step configuration instructions. This section provides general information on the configuration options available within this screen.

Figure 5-3 AAA External Web Server Screen

You can configure the following options from this screen (see [External Authentication > Configuration Instructions](#) for detailed step-by-step instructions for setting up the AP to communicate with an External Web Server):

- **Secret Key:** A password shared by the External Web Server and the AP. This field is reserved for future use.
- **IP Address:** The IP address of the External Web Server.
- **External Login Page URL:** The login page on the external server to which the AP will redirect unauthenticated customers.

Public Space Parameters

AAA Services with the Internal Web Server (IWS)

This screen lets you set the configuration options when authorizing subscribers using the IWS (that is, when **PublicSpace > AAA > Basic > Authentication Method** is set to **Internal**). The IWS is “flushed” into the system’s memory and the subscriber’s login page is served directly from the AP-2500.



NOTE

See [Internal Authentication](#) for information on the internal authentication process and for step-by-step configuration instructions. This section provides detailed information on the configuration options available within this screen.

- [Secure Socket Layer \(SSL\)](#)
- [Portal Page](#)
- [Smart Client](#)
- [User Name & New Subscribers](#)
- [Credit Card Services](#)

ICC SMTP Passthrough Bandwidth Mgmt

HPR AAA Logging URLFilter

Basic External Internal

This tab is used to configure AAA using the Internal Web Server.

Note: Reboot is required everytime SSL support is enabled or disabled. If SSL support is enabled, digital certificates must be obtained to create HTTPS pages. New Subscribers feature must be enabled before enabling the credit Card Service.

Enable SSL ☐ Certificate DNS Name

Enable Portal Page ☐ Portal Page URL

Enable Smart Client ☐

Enable User Name ☒

Enable New Subscribers ☒

Enable Credit Card Service ☒

Credit Card Server URL

Credit Card Server IP (Needs to be in IP Passthrough)

Merchant ID

OK Cancel

Figure 5-4 AAA Internal Web Server Screen

Secure Socket Layer (SSL)

The AP-2500 supports Secure Socket Layer (SSL) to provide end-to-end encrypted links between the AP and subscribers using HTTPS pages. HTTPS stands for *Hypertext Transfer Protocol over Secure Socket Layer*; it is a protocol built into Web browsers that encrypts and decrypts user page requests as well as the pages that are returned by a Web server.

When enabled, SSL protects the information exchanged between your subscribers and the AP (this is particularly important if you authenticate subscribers based on User Name and Password via RADIUS).

Enabling SSL is a two-part process. First, you need to create two SSL keys and locate a third key, which is provided on the AP's CD. Once you have the keys, you can download them to the AP and configure the SSL parameters.

Public Space Parameters

Creating SSL Keys

You need to download three keys to the AP-2500 before enabling SSL. You must create two of these keys yourself: a Private Key file (**cakey.pem**) and a Public Key file (**server.pem**). Proxim provides the third key (**cacert.pem**), on the AP's CD in the **SSL_KEY** folder (it is also included with software updates posted on Proxim's Web site).

To create **cakey.pem** and **server.pem**, you must contact a Certification Authority (CA). Many companies offer certification services. Each CA has its own set of qualification requirements that a company must meet before the CA will grant an SSL certificate. Proxim recommends that you use a well-known CA, such as Verisign (<http://www.verisign.com/>). Refer to Verisign's Web site for more information on SSL and obtaining an SSL certificate.

⇒ NOTE

As of the release of this document, Verisign provides free trial SSL certificates for testing purposes. See Verisign's Web site for details.

The following steps provides an overview of how to create **cakey.pem** and **server.pem**:

1. Download and install **Cygwin** from the Internet. It is available as a free download at several Web sites including <http://www.cygwin.com/>.
 - Cygwin is a UNIX environment for Windows. It operates on computers running Windows 95 and later (except Windows CE).
 - Download and execute the Cygwin **Setup.exe** file. Follow the on-screen instructions to install the software.
 - When prompted to select packages to install, select **cygwin** and **openssl** only. You do not need to install any other packages (in other words, you can skip them).
 - You will use the **openssl** program to generate keys.
2. Locate or generate five large random files and rename them **a.dat**, **b.dat**, **c.dat**, **d.dat**, and **e.dat**.
 - These files are used to seed the random number generator.
 - These files can be any file type (such as Word, Excel, etc.) but you should change the file names to ".dat" as described above (**a.dat** through **e.dat**). Verisign recommends using large compressed log files.
 - The files can have any name but must follow standard DOS naming conventions (that is, a file name with a maximum of eight characters, a period, and a three-character extension).
3. Copy or move these five **dat** files to the directory where **openssl.exe** is installed (typically **c:\cygwin\bin**).
4. Open an MS-DOS command prompt.
5. Use the **cd** command to open the directory that contains **openssl.exe** and the five random files.
 - If the files are installed at **c:\cygwin\bin**, the command prompt should read:
C:\CYGWIN\BIN>
6. Type the following command and press **Enter** to generate a private key with the name **cakey.pem**:
openssl genrsa -rand file1:file2:file3:file4:file5 1024 > cakey.pem
 - **genrsa** is the OpenSSL command to generate a private key.
 - **-rand** is followed by the name of the five random files (include file name extensions and separate files by colons); this argument specifies the names of the files containing random data for the random number generator.
 - **1024** is the size of the private key to generate in bits.
 - **> cakey.pem** specifies the name of the output files.
 - Due to buffer size limitations, the line length should not exceed 80 characters.
 - Do not encrypt the key with any encryption options (such as **-des**, **-des3**, or **-idea**).
 - See <http://www.openssl.org/> for more information on this command.
7. Type the following command and press **Enter** to generate a Certificate Signing Request (CSR):
openssl req -new -key cakey.pem > server.csr
 - **req** is the OpenSSL command to generate a certificate request.
 - **-new** specifies that this command will generate a new certificate request.
 - **-key cakey.pem** specifies the file that contains the private key you generated in the previous step.
 - **> server.csr** specifies the name of the output files.
 - See <http://www.openssl.org/> for more information on this command.

Public Space Parameters

8. When prompted, follow the on-screen instructions and enter the information requested (such as your company's name and address).
 - You will be prompted to enter a **Common Name**. The Common Name is typically composed of the Host name and Domain Name (taking the form of "www.company.com" or "ssl.company.com"). SSL certificates from a CA are specific to the Common Name to which they have been issued at the Host level. You will configure the AP to use this same Common Name.
 9. Provide the Certificate Signing Request (CSR) to your CA to obtain an SSL certificate.
 - Refer to your CA's Web site for details. If you are using Verisign, you can submit the CSR on-line, as outlined in the steps below.
 1. Go to <http://www.verisign.com/>.
 2. Select the **SSL Site Security** or **SSL Certificate** option.
 3. Select the option to **Secure your Web site with Secure Site Services**.
 4. Review the documentation provided by Verisign. Verisign provides information on SSL certificate and step-by-step instructions.
 5. You can skip the step which describes how to create a CSR since you have already created the file.
 6. Open the **server.csr** file you generated with a text editor (such as Notepad) and copy and paste the text to Verisign's on-line form.
 - Begin copying at the "—BEGIN NEW CERTIFICATE REQUEST—" line.
 - Copy through and including the "—END NEW CERTIFICATE REQUEST—" line.
 7. Follow the remaining instructions to complete the enrollment process.
 - If the CA asks you to select your server software vendor when uploading the CSR file, select **Apache Freeware** or **Apache SSL**.
 - You can purchase either a 40-bit or 128-bit key. 128-bit is more secure than 40-bit but many older browsers only support 40-bit.
 - It can take up to a week for the CA to send you the SSL certificate.
 10. After you have received the SSL certificate from the CA, use a text editor (such as Notepad) to open the file.
 11. Copy and paste the Public Key information into a new file.
 - Begin copying at the "—BEGIN CERTIFICATE —" line.
 - Copy through and including the "—END CERTIFICATE —" line.
 12. Save this new file with the filename **server.pem**.
- You have now created two of the three key files required to enable SSL on the AP-2500. The third key file (**cacert.pem**) is included on the AP's CD and with software updates posted on Proxim's Web site.

Enabling SSL on the AP-2500

1. Login to the AP's Web browser.
2. Launch your TFTP server application (if not already running).
3. Copy **cacert.pem**, **cakey.pem**, and **server.pem** to the TFTP server's root directory.
 - If you are using the SolarWinds TFTP program, the root directory is mostly likely *C:\TFTP-Root*.
 - Proxim provides **cacert.pem** on the AP's CD and with software updates posted on Proxim's Web site.
 - You must create your own **cakey.pem** and **server.pem** files. See [Creating SSL Keys](#) for details.
4. Click **Commands > Download**.
5. Enter the IP address of the computer running the TFTP server application in the **Server IP Address** field.
6. Enter **cacert.pem** in the **File Name** field.
7. Set **File Type** to **Generic**.
8. Set **File Operation** to **Download**.
9. Click **OK**.
 - Result: The TFTP operation begins. A new **TFTP Operation Status** window opens.
10. Click **Close** after the TFTP operation is complete.
11. Enter **cakey.pem** in the **File Name** field.
12. Set **File Type** to **Generic**.
13. Set **File Operation** to **Download**.

Public Space Parameters

14. Click **OK**.
 - Result: The TFTP operation begins. A new **TFTP Operation Status** window opens.
15. Click **Close** after the TFTP operation is complete.
16. Enter **server.pem** in the **File Name** field.
17. Leave **File Type** set to **Generic**.
18. Set **File Operation** to **Download & Reboot**.
19. Click **OK**.
 - Result: The TFTP operation begins. A new **TFTP Operation Status** window opens.
20. Click **Close** after the TFTP operation is complete. The AP will reboot automatically.
21. Wait for the AP to finish rebooting.
22. Click **PublicSpace > AAA > Internal**.
23. Place a check mark in the **Enable SSL** box.
24. Enter the Common Name that you used when generating the CSR into the **Certificate DNS Name** box.
 - The Common Name is the name you specified when creating the CSR file.
25. Click **OK**.
26. Reboot the AP.

Notes concerning SSL

- When a subscriber connects to an AP that has SSL enabled, the AP's internal login pages are sent as secure HTTPS pages.
- The AP uses port 1111 for standard logins and port 1112 for secure logins.
- If you are setting up a portal page, a standard login link uses the following syntax:
http://APIADDR:1111/usg/login?OS=http://www.anyWebSite.com/
A secure login link uses the following syntax:
http://[Certificate DNS Name]:1112/usg/login?OS=http://www.anyWebSite.com/
See [Portal Page](#) for more information.

Portal Page

A Portal Page is a great way to customize the login experience for the users at your hotspot. You can provide custom content on the page and links to free Web sites (the list of free Web sites is known as a "walled garden"). For example, an airport restaurant might want to provide free access to the airline Web sites so customers can check their flight status.

However, using a portal page requires more equipment and some Web design skills to implement. Before enabling the Portal Page feature, note the following:

- You must have an external Web server on your network that can host the Portal Page for you. One of the most common Web server application is Microsoft's Internet Information Services (IIS), which is included with Windows 2000 Server.
- You will need to setup the Web server before you can use the Portal Page features.
- You will need to design your own Portal Page (using HTML or a Web design application). Depending on the features that you want to offer, you may also want to design your own Home Page Redirection page.
 - The Portal Page can be as simple as an HTML document that has links to the AP's login screen and to your walled garden content.

The following diagram illustrates a network topology using the AP's Internal Web Server with a portal page:

Public Space Parameters

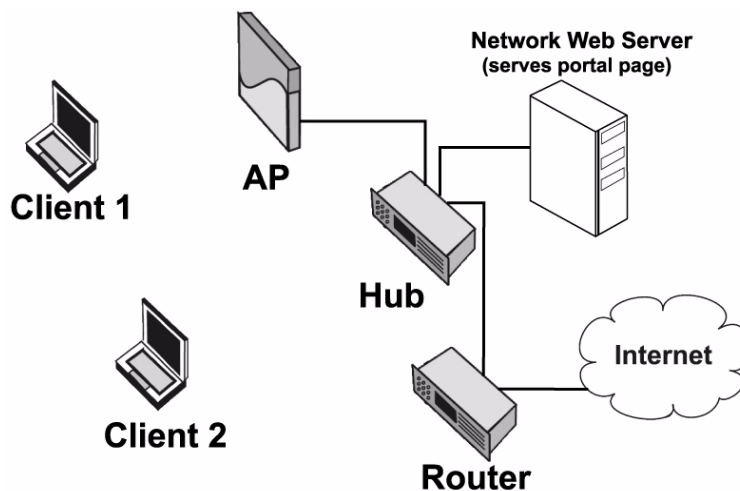


Figure 5-5 Internal Authentication with Portal Page

The following sections provide basic instructions for using a Portal Page.

Setting up a Web Server (Microsoft IIS)

If you have a Windows 2000 Server, follow these basic steps to setup the IIS Web server.



NOTE

For detailed information, refer to Windows 2000's on-line Help documentation. If you want to use a different Web server program, follow the installation instructions provided with the program.

1. Confirm that IIS is not already installed.
 - Click **Start > Programs > Administrative Tools**.
 - If the list of tools includes the **Internet Services Manager**, IIS is installed. Proceed to Step 7.
 - If the Internet Services Manager is not listed, IIS is not yet installed. Proceed to Step 2.
2. Click **Start > Control Panel**.
3. Double-click the **Add/Remove Programs** icon.
4. Click the **Add/Remove Windows Components** option.
5. Place a check mark next to the **Internet Information Services (IIS)** option.
 - This procedure assumes that you will be installing all of the default IIS options. See the Windows 2000 documentation if you have a question concerning a particular option.
6. Click **Next** and follow the on-screen instructions to install IIS.
 - You may be prompted to insert your Windows 2000 installation CD during the installation process.
7. Launch the **Internet Services Manager** from **Start > Programs > Administrative Tools**.
8. Click the plus sign to the left of the server icon (located in the frame on the left side of the window).
9. Right-click the **Default Web Site** option and choose **Properties** from the drop-down list.
10. Click the **Home Directory** tab and enter the local path for the Web site files.
 - If you use the default settings, the path should be `c:\inetpub\wwwroot`.
 - Note the location of the Web site files. You will need to put the Portal Page files in this directory later.
11. Click **OK** to close the manager window.
 - Refer to the Windows 2000 documentation if you want to configure the other Web server features.
12. Open a Command Prompt from **Start > Programs > Accessories**.
13. Type **ipconfig** and press **Enter**.
14. Note the Server's IP address. You will need this information later when configuring the Portal Page parameters.

Public Space Parameters

Designing a Portal Page

A Portal Page is a Web page; you can design it using whatever Web design tools you have available. The Portal Page does not have to be very complicated. At its most basic, the Portal Page needs a link to the AP's Login page.

The AP's standard Internal Login page is located at:

`http://APIADDR:1111/usg/login?OS=http://www.anyWebSite.com/`

where:

- **APIADDR** is the AP's IP address
 - Some portal pages can obtain the AP's IP address automatically from the redirected HTTP request (such as the ASP sample pages provided with the AP). See [Enabling the AP-2500 to Use a Portal Page > ASP](#) for an example.
- **www.anyWebSite.com** is any Web site that you choose
 - The AP-2500 needs an Origin Server (OS) statement to function properly. Typically this would be the user's default home page or requested page but if you are using plain HTML, you must specify a URL for the Portal Page to work properly. The HTML sample file uses *www.yahoo.com*.
 - In general, this should be a Web site that you want to direct your customers to after successful login (similar to the [Home Page Redirection \(HPR\)](#) feature).

NOTE

If you enabled [Secure Socket Layer \(SSL\)](#), the secure Login page is located at:

`http://[Certificate DNS Name]:1112/usg/login?OS=http://www.anyWebSite.com/`

Proxim provides two sample Portal Pages for the AP-2500 to help hotspot operators who have limited Web design experience get started. These sample pages are in the CD's *Docs/samples/* folder. Alternatively, you can download the sample pages from Proxim's Web site at <http://www.proxim.com/>.

The first sample page is an HTML file called *portalpage.html*. This is a Portal Page at its most basic. This page is suitable if you plan to use **Home Page Redirection** to direct subscribers to a specific Web site following successful authentication. With this option, your customer is not automatically returned to his browser's default home page.

The second sample contains two Active Server Page (ASP) files: *portalpage.asp* and *confirm.asp*. Microsoft's IIS uses this file type; the ASP files contain script commands that are processed by the IIS server. You can use these files if you use Microsoft IIS and you want to incorporate some additional features, namely:

- Redirect customers back to the Web site they initially requested before viewing the Portal Page (typically their browser's home page).
- Provide User Name and Password fields on your Portal Page so customers can login directly from that screen.
 - This feature uses a Form to send the User Name and Password information to the AP (HTTP POST command). The User Name/Password form uses the following syntax to create a **User Name** field, a **Password** field, and a **Submit** button on a Web page:

```
<FORM name=member
action="http://<%=request("IP")%>:1111/usg/process?OS=<%=request("?OS")%>&" method="POST">
<p> <b>Enter your Username :</b> <input type="text" name="username" size="20"> </p>
<p> <b>Enter your Password :</b> <input type="password" name="password" size="20"> </p>
<p> <INPUT TYPE="submit" VALUE="Submit Query"> </p>
</FORM>
```

 - **`<%=request("IP")%>`** notifies an IIS server to parse out the AP's IP address from the HTTP redirect request.
 - **`<%=request("?OS")%>`** notifies an IIS server to parse out the subscriber's original request from the HTTP redirect request.
 - Refer to the *portalpage.asp* file for more information.

NOTE

Proxim also provides a sample Perl file on the installation CD. This file offer similar features to the *portalpage.asp* file but can be used with any Web server that supports Perl scripts. This file is intended for advanced users who have experience with Perl. If you want to use the Perl sample, follow the instructions below for the ASP pages. However, note that the Perl sample does not include an equivalent to *confirm.asp*. Also, you must have a Perl application installed on your server and the folder on your Web server that will contain the Perl file must be configured to execute Perl scripts that use a .pl extension.

Public Space Parameters

Deciding which sample is right for your hotspot depends on the customer experience you want to provide. The sections below describe how the customer interacts with the AP-2500 under the following scenarios:

- [No Portal Page](#)
- [HTML Portal Page](#)
- [ASP Portal Pages](#)

No Portal Page

1. Customer enters the hotspot and turns on his Wi-Fi enabled computer.
2. The customer's computer connects to the AP wirelessly.
3. The customer launches a Web browser.
4. The Web browser attempts to load the customer's default home page (such as <http://www.yahoo.com/>) but is redirected to the AP's internal login screen.
5. The AP's internal login screen appears. The customer does not have access to free "walled garden" content (or at least the customer has no knowledge that free content is available).
6. The customer follows the on-screen instructions and successfully logs in or signs up for service.
7. Following successful authentication, the customer is redirected to the Web page he originally request or to whatever page you specified in the **Home Page Redirection URL** field (if enabled; see [Home Page Redirection \(HPR\)](#)).
8. The Information and Control Console (ICC) Java applet opens a second, small window on the customer's desktop, if enabled.

HTML Portal Page

1. Customer enters the hotspot and turns on his Wi-Fi enabled computer.
2. The customer's computer connects to the AP wirelessly.
3. The customer launches a Web browser.
4. The Web browser attempts to load the customer's default home page (such as <http://www.yahoo.com/>) but is redirected to your Portal Page.
5. The customer can browse free "walled garden" content listed on the Portal Page or click a link to login for full access.
6. The customer wants full access so he clicks the link to login. The AP's internal login screen appears.
7. The customer follows the on-screen instructions and successfully logs in or signs up for service.
8. Following successful authentication, the customer is redirected to the page you specified in the <http://APIPADDR:1111/usg/login?OS=http://www.anyWebSite.com/> statement in the HTML portal page file or to whatever page you specified in the **Home Page Redirection URL** field (if enabled; see [Home Page Redirection \(HPR\)](#)).
9. The Information and Control Console (ICC) Java applet opens a second, small window on the customer's desktop, if enabled.

ASP Portal Pages

1. Customer enters the hotspot and turns on his Wi-Fi enabled computer.
2. The customer's computer connects to the AP wirelessly.
3. The customer launches a Web browser.
4. The Web browser attempts to load the customer's default home page (such as <http://www.yahoo.com/>) but is redirected to your Portal Page.
5. The customer can browse free "walled garden" content listed on the Portal Page or click a link to login for full access.
6. The customer wants full access so he logs into the AP using one of the following methods:
 - Customer enters his User Name and Password in the fields provided on the portal page and clicks **Submit**.
 - Customer clicks a link provided on the portal page that sends the customer to the AP's internal login screen.

Public Space Parameters

7. Following successful authentication, the customer is redirected to the page he originally requested or to the page you specified in the **Home Page Redirection URL** field (if enabled; see [Home Page Redirection \(HPR\)](#)).
 - You can use the *confirm.asp* sample page to display a second custom screen that can provide additional information to your subscribers following successful authentication. The customer can then click a link on the confirmation screen to be redirected to his originally requested page after reviewing the information on the *confirm.asp* page.
8. The Information and Control Console (ICC) Java applet opens a second, small window on the customer's desktop, if enabled.
9. If using a custom HPR page like *confirm.asp*, the customer clicks a button provided on that page that redirects his browser to the page he originally requested (or to that site's default Web page; see the discussion on **Parameter Passing** at [Home Page Redirection \(HPR\)](#) for details).

Editing the Sample Portal Page Files

HTML

To edit the sample HTML Portal Page file, simply open the file using a text editor, such as Notepad.

1. Open the *portalpage.html* file with in Notepad.
2. Replace the two *APIADDR* statements with the IP address of your AP-2500.
3. Edit the "Free Content" section as necessary. Each free content link in the bullet list should have the following syntax:

```
<LI><a href="http://www.anyURL.com/">Description for Any URL Site</a>
```

4. Save your changes and close the file.

ASP

To edit the sample ASP Portal Page file, simply open the file using a text editor, such as Notepad. You only need to edit the walled garden content in the ASP file; you do not need to specify the IP address of your AP; this information will be transmitted by the AP in the redirect request.

1. Open the *portalpage.asp* file with in Notepad.
2. Edit the "Free Content" section as necessary. Each free content link in the bullet list should have the following syntax:

```
<LI><a href="http://www.anyURL.com/">Description for Any URL Site</a>
```

3. Save your changes and close the file.



NOTE

For the sample procedure described in this document, you do not need to edit the *confirm.asp* file.

Enabling the AP-2500 to Use a Portal Page

Refer to the steps below that correspond to the sample files you have selected.

HTML

1. Copy the two sample files (*portalpage.html* and *portalogo.gif*) to a folder on your Web server. For this example, the files are copied to *c:\inetpub\wwwroot\portal*.
2. Configure the AP to use Internal Authentication, following the instructions described in the [Internal Authentication](#) section. Skip any steps that refer to Portal Page, walled garden, or Home Page Redirection.
3. Click **PublicSpace > AAA > Internal**.
4. Place a check mark in the **Enable Portal Page** field.
5. Enter the location of the *portalpage.html* file in the **Portal Page URL** field.
 - In the example below, the Web server's IP address is 192.168.0.101. Therefore, the **Portal Page URL** field reads: **http://192.168.0.101/portal/portalpage.html**.

Public Space Parameters

The screenshot shows the Proxim Wireless Networks configuration interface. On the left is a sidebar with buttons: Status, Configure, Monitor, Commands, PublicSpace (highlighted), Subscriber, Help, and Exit. The main area has tabs: ICC, SMTP, Passthrough, Bandwidth Mgmt, HPR, AAA (highlighted), Logging, and URLFilter. Under the AAA tab, there are sub-tabs: Basic, External, and Internal (highlighted). The Internal tab contains the following configuration options:

This tab is used to configure AAA using the Internal Web Server.

Note: Reboot is required everytime SSL support is enabled or disabled. If SSL support is enabled, digital certificates must be obtained to create HTTPS pages. New Subscribers feature must be enabled before enabling the credit Card Service.

Enable SSL	<input type="checkbox"/>	Certificate DNS Name	<input type="text" value="ssl.myhotspot.com"/>
Enable Portal Page	<input checked="" type="checkbox"/>	Portal Page URL	<input type="text" value="http://192.168.0.101/port"/>
Enable Smart Client	<input type="checkbox"/>		
Enable User Name	<input checked="" type="checkbox"/>		
Enable New Subscribers	<input checked="" type="checkbox"/>		
Enable Credit Card Service	<input checked="" type="checkbox"/>		
Credit Card Server URL	<input type="text" value="https://secure.authorize.n"/>		
Credit Card Server IP	<input type="text" value="206.253.210.201"/>	<i>(Needs to be in IP Passthrough)</i>	
Merchant ID	<input type="text" value="myid"/>		

At the bottom are OK and Cancel buttons.

Figure 5-6 Portal Page Configuration

6. Click the **Passthrough** tab.
7. Place a check mark in the **Enable Passthrough Address** box, if necessary.
8. Add the DNS names for the Web sites in your walled garden to the **Passthrough DNS Table**.
 - Click **Add**.
 - Enter the DNS name in the field provided.
 - Click **OK**.
 - Continue entering DNS names and clicking **OK** until you have entered all of the Web sites in your walled garden.
 - Click the back arrow button to return to the previous screen.
9. Add the IP address of your Web server to the **Passthrough IP Table**.
 - Click **Add**.
 - Enter the Web server's IP address in the field provided.
 - Click **OK**.
 - Click the back arrow button to return to the previous screen.

Public Space Parameters

The screenshot shows a configuration window for 'Public Space Parameters'. At the top, there is a checkbox labeled 'Enable Passthrough Address' which is checked. Below this are two sections: 'Passthrough DNS Table' and 'Passthrough IP Table'. Each section has 'Add' and 'Edit' buttons. The DNS table lists three domains: tvguide.com, weather.com, and coffeeuniverse.com, all with a status of 'Active'. The IP table lists two IP addresses: 206.253.210.201 and 192.168.0.101, both with a status of 'Active'.

Passthrough DNS Table	
DNS Names	Status
tvguide.com	Active
weather.com	Active
coffeeuniverse.com	Active

Passthrough IP Table	
IP Address	Status
206.253.210.201	Active
192.168.0.101	Active

Figure 5-7 Sample Passthrough Tables

10. Click **OK**.
11. Click the **HPR** tab.
12. Place a check mark in the **Enable Home Page Redirection** box.
13. Enter the Web site to which you want to direct customers following successful authentication in the **Redirection URL** field (for example, <http://www.yahoo.com/>).
14. Click **OK**.
15. Click **Commands > Reboot**.
16. Click **OK** to reboot the AP so your changes will take effect.
17. Test the Portal Page feature by turning on a wireless computer and launching its Web browser.
 - Note that the computer must not be a current or active subscriber (that is, the wireless card's MAC address cannot appear in the [Authorized Subscribers](#) Table or in the [Current Subscribers Table](#) with **State** sent to **Valid**) for this test to work properly.
 - A successful test should follow the procedure described for the HTML file in [HTML Portal Page](#).

ASP

1. Copy the three sample files (*portalpage.asp*, *confirm.asp*, and *portalogo.gif*) to a folder on your Web server. For this example, the files are copied to `c:\inetpub\wwwroot\portal\`.
2. Configure the AP to use Internal Authentication, following the instructions described in the [Internal Authentication](#) section. Skip any steps that refer to Portal Page, walled garden, or Home Page Redirection.
3. Click **PublicSpace > AAA > Internal**.
4. Place a check mark in the **Enable Portal Page** field.
5. Enter the location of the *portalpage.asp* file in the **Portal Page URL** field and include the AP's IP address in a **?IP=APIPADDR&** statement at the end of the file name.
 - In the example below, the Web server's IP address is 192.168.0.101 and the AP's IP address is 192.168.0.4. Therefore, the **Portal Page URL** field reads: **`http://192.168.0.101/portal/portalpage.asp?IP=192.168.0.4&`**.
 - Using the above example, the URL in the subscriber's Web browser would read as follows after a successful redirect (assuming that the customer attempted to access the Yahoo home page before logging in):
`http://192.168.0.101/portal/portal.asp?IP=192.168.0.4?OS=http://www.yahoo.com/`
 - The Web server parses out the IP and OS statements from the URL string based on the instructions in the ASP file (the `<%=request("IP")%>` and `<%=request("OS")%>` commands).

Public Space Parameters

The screenshot shows the Proxim Wireless Networks configuration interface. On the left is a sidebar with buttons: Status, Configure, Monitor, Commands, **PublicSpace** (highlighted), Subscriber, Help, and Exit. The main area has tabs: ICC, SMTP, Passthrough, Bandwidth Mgmt, HPR, **AAA** (highlighted), Logging, and URLFilter. Under the AAA tab are sub-tabs: Basic, External, and **Internal** (highlighted). The Internal tab contains the following configuration options:

This tab is used to configure AAA using the Internal Web Server.

Note: Reboot is required everytime SSL support is enabled or disabled. If SSL support is enabled, digital certificates must be obtained to create HTTPS pages. New Subscribers feature must be enabled before enabling the credit Card Service.

Enable SSL	<input type="checkbox"/>	Certificate DNS Name	<input type="text" value="ssl.myhotspot.com"/>
Enable Portal Page	<input checked="" type="checkbox"/>	Portal Page URL	<input type="text" value="http://192.168.0.101/port"/>
Enable Smart Client	<input type="checkbox"/>		
Enable User Name	<input checked="" type="checkbox"/>		
Enable New Subscribers	<input checked="" type="checkbox"/>		
Enable Credit Card Service	<input checked="" type="checkbox"/>		
Credit Card Server URL	<input type="text" value="https://secure.authorize.n"/>		
Credit Card Server IP	<input type="text" value="206.253.210.201"/>	<i>(Needs to be in IP Passthrough)</i>	
Merchant ID	<input type="text" value="myid"/>		

At the bottom are **OK** and **Cancel** buttons.

Figure 5-8 Portal Page Configuration

6. Click the **Passthrough** tab.
7. Place a check mark in the **Enable Passthrough Address** box, if necessary.
8. Add the DNS names for the Web sites in your walled garden to the **Passthrough DNS Table**.
 - Click **Add**.
 - Enter the DNS name in the field provided.
 - Click **OK**.
 - Continue entering DNS names and clicking **OK** until you have entered all of the Web sites in your walled garden.
 - Click the back arrow button to return to the previous screen.
9. Add the IP address of your Web server to the **Passthrough IP Table**.
 - Click **Add**.
 - Enter the Web server's IP address in the field provided.
 - Click **OK**.
 - Click the back arrow button to return to the previous screen.

Public Space Parameters

Enable Passthrough Address ☒

Passthrough DNS Table

AddEdit

DNS Names	Status
tvguide.com	Active
weather.com	Active
coffeeniverse.com	Active

Passthrough IP Table

AddEdit

IP Address	Status
206.253.210.201	Active
192.168.0.101	Active

Figure 5-9 Sample Passthrough Tables

10. Click **OK**.



NOTE

If you disable Home Page Redirection, your subscribers will be automatically redirected to the page they originally requested (following successful authentication). The instructions below describe how to enable Home Page Redirection; when used in conjunction with the `confirm.asp` file, this demonstrates how you can direct customers to a customized confirmation page after successful authentication that you can use to provide additional information to your subscribers.

11. Click the **HPR** tab.

12. Place a check mark in the **Enable Home Page Redirection** box.

13. Place a check mark in the **Enable Parameter Passing** box.

- This feature allows the AP-2500 and your Web server to remember a subscriber's Origin Server (OS) request. However, note that the AP may truncate the subscriber's request to the site's default Web page. See [Home Page Redirection \(HPR\)](#) for details.
- Your subscribers will be redirected to the site they originally requested if you disable HPR and do not use the `confirm.asp` file (in other words, the AP will not truncate the requested URL).

14. Enter the location of the `confirm.asp` file in the **Redirection URL** field.

- In the example below, the Web server's IP address is 192.168.0.101. Therefore, the **Redirection URL** field reads: **`http://192.168.0.101/portal/confirm.asp`**.

Public Space Parameters

ICC SMTP Passthrough Bandwidth Mgmt

HPR AAA Logging URLFilter

Status
Configure
Monitor
Commands
PublicSpace
Subscriber
Help
Exit

This tab is used to configure Home Page Redirection (HPR). HPR, if enabled, redirects subscribers browser to the specified URL.

Note: DNS must be properly configured to enter URLs instead of numeric IP addresses. If HPR is enabled, URL for the redirected home page must be entered.

Home Page Redirection Configuration

Enable Home Page Redirection ☒

Enable Parameter Passing ☒

Redirection URL
URL needs protocol field. eg. http://www.proxim.com/

Redirection Frequency Mins

OK Cancel

Figure 5-10 HPR (with Parameter Passing)

15. Click **OK**.
16. Click **Commands > Reboot**.
17. Click **OK** to reboot the AP so your changes will take effect.
18. Test the Portal Page feature by turning on a wireless computer and launching its Web browser. Note that the computer must not be a current or active subscriber (that is, the wireless card's MAC address cannot appear in the Authorized Subscribers Table or the Current Subscribers Table) for this test to work properly.
 - Note that the computer must not be a current or active subscriber (that is, the wireless card's MAC address cannot appear in the [Authorized Subscribers](#) Table or in the [Current Subscribers Table](#) with **State** sent to **Valid**) for this test to work properly.
 - A successful test should follow the procedure described for the ASP files in [ASP Portal Pages](#).

Smart Client

The AP-2500 supports the connection software for three hotspot aggregators:

- Boingo -- <http://www.boingo.com/>
- GRIC -- <http://www.gric.com/>
- iPass -- <http://www.ipass.com/>

These companies provide customers with wireless access at hotspots across the country. At each specific hotspot, the aggregator may own the access infrastructure or they may have an agreement in place with the hotspot operator.

Refer to the Web sites listed above if you are interested in partnering with a hotspot aggregator. This type of agreement allows you to use the aggregator's name to promote your hotspot and reduces your setup and maintenance costs (the aggregator handles customer billing and pays you a fee each time a subscriber logs in from your hotspot).

If you are already a partner with one of these companies, you should enable the **Smart Client** option so the AP-2500 can communicate with the aggregator's end-user application. This application is installed on a subscriber's computer and facilitates login and connection to the aggregator's services. (For example, a Boingo customer can use his Boingo application to login to his account through the AP.)

The following diagram illustrates the network layout for this type of configuration.

Public Space Parameters

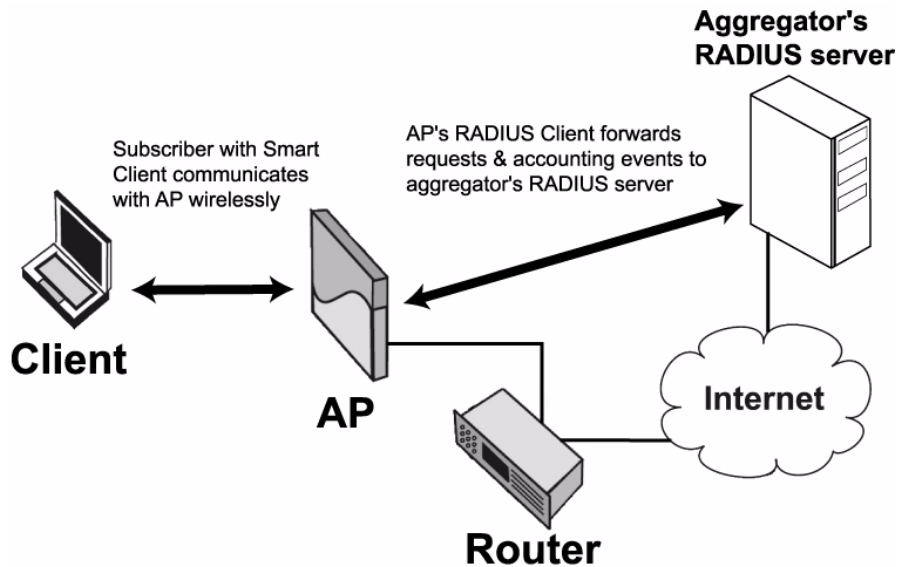


Figure 5-11 AP Communicating with Hotspot Aggregator

The following steps describe how you should configure the AP-2500 if you are partnered with a hotspot aggregator:

1. Follow the installation steps described in [Internal Authentication](#) and [Internal Authentication with RADIUS](#).
 - Configure the RADIUS Authentication and Accounting settings as required by your hotspot aggregator.
 - In general, the aggregator should supply you with the settings of a RADIUS server on the Internet that performs AAA functions for the aggregator's subscribers.
2. Click **PublicSpace > AAA > Internal** to update the **AAA Internal Web Server** options so they match the following settings (if necessary):
 - Place a check mark in the **Enable SSL** box and enter the **Certificate DNS Name** (this is optional but recommended to provide subscribers with a secure login).
 - If using SSL, you must download keys to the AP first. See [Secure Socket Layer \(SSL\)](#).
 - Place a check mark in the **Enable Portal Page** box and enter the page's location in the **Portal Page URL** field if you want to provide a custom login page to subscribers.
 - See [Portal Page](#).
 - You must also enter the portal page address in the [Passthrough Addresses](#) table.
 - Place a check mark in the **Enable Smart Client** box.
 - Place a check mark in the **Enable User Names** box.
 - Remove the check mark from the **Enable New Subscribers** box (that is, disable support for new subscribers).
 - Remove the check mark from the **Enable Credit Card Services** box (that is, disable credit card services).

Public Space Parameters

ICC SMTP Passthrough Bandwidth Mgmt

HPR AAA Logging URLFilter

Status

Configure

Monitor

Commands

PublicSpace

Subscriber

Help

Exit

Basic External Internal

This tab is used to configure AAA using the Internal Web Server.

Note: Reboot is required everytime SSL support is enabled or disabled. If SSL support is enabled, digital certificates must be obtained to create HTTPS pages. New Subscribers feature must be enabled before enabling the credit Card Service.

Enable SSL ☒ Certificate DNS Name ssl.myhotspot.com

Enable Portal Page ☒ Portal Page URL http://205.23.12.41/subsc

Enable Smart Client ☒

Enable User Name ☒

Enable New Subscribers ☐

Enable Credit Card Service ☐

Credit Card Server URL https://secure.authorize.n

Credit Card Server IP 205.253.210.201 (Needs to be in IP Passthrough)

Merchant ID

OK Cancel

Figure 5-12 AAA Internal Settings if Enabling Smart Client

3. Click **OK** to save the settings.
4. Reboot the AP.

User Name & New Subscribers

The **User Name** and **New Subscribers** options work in conjunction to determine who can connect to the Internet and what credentials the AP uses to authenticate users.

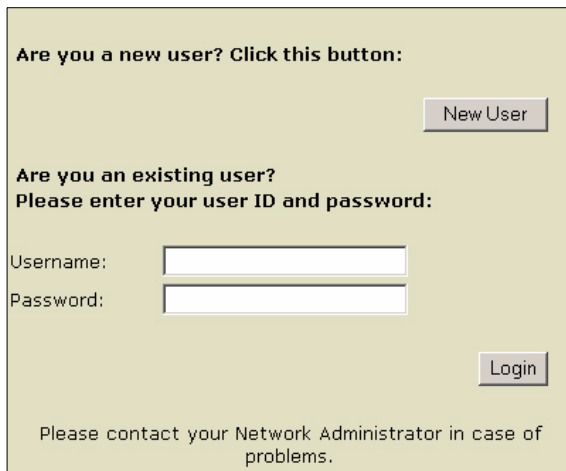
The following table summarizes the available User Name and New Subscribers combinations:

User Name	New Subscribers	System Response
Disabled (default)	Enabled (default)	Allows new and existing subscribers access to the network without supplying a User name and password. Authentication is based on the MAC address of the subscriber's Wi-Fi card. This setting works in conjunction with credit card services.
Enabled	Enabled	Allows new and existing subscribers access to the network after supplying a user name and password. This setting works in conjunction with credit card services.
Enabled	Disabled	Only allows existing subscribers (either in a RADIUS database or in the Authorized Subscribers Table) after supplying a user name and password.
Disabled	Disabled	Only allows existing subscribers in the Authorized Subscribers Table based on a card's MAC address.

Table 5-1 User Name and New Subscriber

When User Name is enabled, the AP displays a **User Name** and **Password** field on its login screen. When New Subscribers is enabled, the AP displays a **New User** button. The following example shows the AP's internal login screen when both options are enabled.

Public Space Parameters



The login screen has a light beige background. At the top, it asks 'Are you a new user? Click this button:' with a 'New User' button to the right. Below this, it asks 'Are you an existing user? Please enter your user ID and password:'. There are two input fields: 'Username:' and 'Password:'. A 'Login' button is positioned to the right of the password field. At the bottom, a note says 'Please contact your Network Administrator in case of problems.'

Figure 5-13 Sample Login Screen Presented to Subscribers

Sample scenarios include:

- If you are renting cards to customers, disable **User Name** and **New Subscribers**. Only cards whose MAC addresses are entered in the Authorized Subscriber Table will have access to the Internet.
- If you are manually entering user names and passwords into the [Authorized Subscribers](#) Table, enable **User Name** but disable **New Subscribers**.
- If you are using credit card services, enable **User Name** and **New Subscribers** (if you want subscribers to create a username and password) or only enable **New Subscribers** (if you want subscribers to access the network based on their wireless card's MAC address).
 - The only difference between these two scenarios is that with username/password, subscribers can access the Internet from a different wireless device at a later date. For example: a subscriber purchases two days of Internet access. On the second day, the subscriber returns to the hotspot with a different wireless card installed. If using username/password authentication, the subscriber will be able to access the Internet using the different card with no intervention from the hotspot operator. Note that the subscriber will only be able to log in using a different wireless card if the account is not already in use (as displayed in the [Current Subscribers Table](#)). Note that a subscriber that has turned off his computer or has left the hotspot is removed from the Current Subscriber Table after 10 minutes.

Credit Card Services

A key payment feature of the AP-2500 is direct Credit Card billing. New subscribers can enter your hotspot and sign up for service directly from their computer and pay for it by credit card. Here's an overview of the process:

1. Customer enters hotspot and turns on laptop.
2. The laptop's wireless radio connects to the AP.
3. Customer opens a Web browser, which attempts to access its home page.
4. The AP automatically redirects the customer to the hotspot's portal page or to the AP's internal login screen.
5. Customer selects **New User** option from login screen.
6. Customer selects account options (user name, password, billing plan, duration of plan, etc.).
7. AP displays a screen that summarizes the customer's selections.
8. Customer clicks the **Purchase** button.
9. AP passes information to credit card service provider's server.

➡ NOTE

All data communications between the credit card server and the AP are encrypted by SSL. The AP never "sees" subscriber credit card numbers.

10. Customer connects to credit card service provider's URL over a secure HTTPS connection.
11. Customer enters credit card information and clicks the **Submit** button.
12. When the transaction has been approved, the credit card service provider's server sends confirmation to AP.

Public Space Parameters

13. AP adds customer to its [Authorized Subscribers Table](#) for the period of time purchased by the customer; the AP also adds the customer to the [Current Subscribers Table](#).
14. AP redirects customer to home page or to page specified by the Home Page Redirection feature.
15. Customer accesses the Internet. If the customer leaves the hotspot and comes back before the time period elapses, the customer can regain access by entering his user name and password when prompted.
16. After the customer's purchased time has expired, customer is redirected back to the login screen to purchase more time (if applicable).

Credit Card Services Requirements

Review the following guidelines and requirements before enabling Credit Card Services on the AP:

- This feature is available if you are using Internal authentication.
- The AP must have a static, routable, public IP address to use credit card billing.
- You need an account with a credit card service provider to use this feature. The AP supports several credit card service companies by default:
 - Datacenter Luxembourg (in Europe) -- <http://www.dclux.com/>
 - ChainFusion (in Asia) -- <http://www.chainfusion.com/>
 - Authorize.net's WebLink solution (U.S.) -- <http://www.authorize.net/>
- As of the release of this documentation, Authorize.net is discontinuing support for WebLink. Proxim is working to provide support for Authorize.net's Simple Integration Solution (SIM) method in the next AP-2500 firmware release.



NOTE

If your credit card service provider is not on the above list, you will need to provide your service provider with the [Credit Card Interface Specification](#). The credit card service provider will need to develop an interface that communicates with the AP-2500 using this specification.

- You will need to configure any account settings required by your credit card service provider. For example, if you are using Authorize.net's WebLink solution, you must add the AP's IP address and port number as a Referrer URL:
 1. Go to <http://www.authorize.net/> and login to your account with your Merchant ID and password.
 2. Click **Settings > WebLink > Referrer URLs**.
 3. Click **Add URL**.
 4. Enter **`http://APIADDR:1111/`** (where *APIADDR* is the AP's IP address)
 - For example: **`http://205.23.43.12:1111/`**
 5. Click **Submit**.
 6. Log out of the Authorize.net account.

Enabling Credit Card Services on the AP

Follow these steps to enable Credit Card billing:

1. Login to the AP's Web browser interface.
2. Click **Configure > Network > IP Configuration**.
3. Confirm that the AP has been assigned a static, routable, public IP address.
4. Click **PublicSpace > AAA > Internal**.
5. Place a check mark in the **Enable Credit Card Services** box.
6. Enter the URL supplied by your credit card service provider. By default, the Authorize.net address appears in the **Credit Card Server URL** field.
7. Enter the IP address for the credit card server. By default, the Authorize.net address appears in this field (**Credit Card Server IP**). You will also need to enter this IP address in the [Passthrough Addresses](#) list.
8. Enter your **Merchant ID** (supplied by your credit card service provider) in the field provided.
9. Click **OK**.
10. Click the **Passthrough** tab.
11. Enter the Credit Card Server IP address in the **Passthrough IP Table**.
12. Reboot the AP.

⇒ NOTE

If you want the AP to send copies of credit card transactions to a mirroring server, see [Credit Card Mirroring](#) for instructions.

Credit Card Mirroring

The AP-2500 can send copies of credit card transaction billing records to external servers that are defined in the **Subscriber > Billing > Mirroring** screen. Also, if the primary and secondary servers are down, the AP-2500 can store up to 2,000 credit card transaction records and send the information to the server when the connection is re-established.

You can define up to three billing servers to which the AP will send billing records: a primary server (required), a secondary server (optional), and a carbon copy server (to create a back-up copy of billing records). The AP attempts to send billing records to the primary server first. If the primary server fails to acknowledge the record, the AP attempts to send the record to the secondary server (based on the **Retransmit Method** setting). The AP also sends records to the carbon copy server immediately after processing; however, the AP does not wait for an acknowledgment from the carbon copy server (that is, the AP never attempts to retransmit messages sent to the carbon copy server).

When there is a billing record in the message queue, the AP performs the following tasks:

1. Stores the billing record in its flash memory.
2. Creates an XML packet, based on the new billing record.
3. Sends the billing record to the carbon copy server.
4. Transmits the data currently stored in the flash to the primary or secondary server based on the specified retransmission method (round robin: A-B-A-B or fail-over: A-A-B-B).

The system stores the billing record in its flash so that the record is not lost if there is a problem during transmission attempts (such as, the AP is powered down unexpectedly).

⇒ NOTE

Billing records are sent to the carbon copy server only after the records are placed in the message queue. Carbon copy servers will not receive the records again even if the AP has to retransmit the data to the primary or secondary server.

Bill Mirroring Server

The AP sends the XML strings that contain the billing information to a specified server's IP address on the specified port. You need a software program installed on your server that will listen for packets from the AP on the specified port. Proxim provides a sample Bill Mirror Server Daemon in the CD's *Docs/samples/* folder. This program is provided for illustration and testing purposes only. It translates the AP's XML strings into plain text. Proxim provides no guarantee that this program will function error-free.

Follow these steps to install the sample bill mirroring software:

1. Copy *sample_bill_mirroring_server.zip* from the CD's *Docs/samples/* folder to a Windows 2000 server.
2. Extract the five files from the ZIP file to a folder on the Windows 2000 server.
 - Among the files are three *.BAT files. These batch files launch the bill mirror daemon.
 - **Primary_4444.bat**: This file is for the primary server. It configures the program to listen on port 4444.
 - **Secondary_4445.bat**: This file is for the secondary server. It configures the program to listen on port 4445.
 - **CC1_4446.bat**: This file is for the carbon copy server. It configures the program to listen on port 4446.
 - You can change the port number by editing the contents of a batch file with a text editor.
3. Execute one of the three batch files to launch the bill mirror daemon so that it listens on the specified port.
 - For example, executing *Primary_4444.bat* will launch the program and it will listen for packets from the AP on port 4444.
4. Configure the AP's Bill Mirroring settings.
 - The server IP address and port parameters must match the server's settings.
 - For example, if you executed *Primary_4444.bat*, configure the **Primary Server IP Address** to match the IP address of your Windows 2000 server and set **Port** to 4444.
5. The AP should now send copies of credit card transactions to the configured servers running the sample bill mirroring software. The server saves these transactions to two log files: *raw.txt* (contains full XML strings) and *log.txt* (contains only the incoming data from the AP). See [XML Packet Format](#) for details.

Public Space Parameters

Enabling Bill Mirroring

Follow these steps to enable bill mirroring:

1. Login to the AP's Web browser interface.
2. Click **Subscriber > Billing > Mirroring**.

Billing Messages Authorized

Options **Mirroring** Plan 0 Plan 1 Plan 2 Plan 3 Plan 4 Plan 5

This tab is used to configure Billing Records Mirroring(BRM) feature. The access point, using BRM feature, can send copies of credit card transaction billing records to external servers defined here.

Credit Card Mirroring

Enable Mirroring ☐

Property ID

Access Point ID

Retransmit Method Alternate ☐ Donot Alternate ☒

Retransmit Attempts

Retransmit Delay

	Primary Server	Secondary Server	CarbonCopy Server
IP	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
URL	<input type="text"/>	<input type="text"/>	<input type="text"/>
Secret Key	<input type="text"/>	<input type="text"/>	<input type="text"/>
Port	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

OK Cancel

Figure 5-14 Credit Card Mirroring Screen

3. Place a check mark in the **Enable Mirroring** box.
4. Enter a Property Identification code in the **Property ID** field.
 - You can define this field as necessary to identify the location of the AP.
5. Enter an AP-2500 Identification code in the **Access Point ID** field.
 - This should be a unique value for each AP. This field differentiates between APs if you have multiple units installed in the same location (that is, with the same **Property ID**).
6. Select a **Retransmit Method** for billing records being sent to the primary (A) or secondary (B) servers:
 - Alternate: This is a round-robin method (e.g., try A, try B, try A, try B)
 - Do Not Alternate: This is the fail-over method (e.g., try A twice, try B twice).
7. Enter the number of **Retransmit Attempts** in the field provided. This value specifies how many times the AP will attempt to transmit the billing record before determining that the transmission has failed.
8. Enter the **Retransmit Delay** (in seconds) in the field provided. This value specifies how long the AP will wait between transmission attempts.

Public Space Parameters

9. Enter the following settings for the primary server, secondary server (if any), and carbon copy server that will receive billing records from the AP:
 - **IP:** Enter the server's IP address in the field provided.
 - **URL:** This field is optional. If a URL is not specified, the AP sends an XML packet to the server's IP address on the selected port. The system administrator decides if the server will listen for the packets on the port or if the packets need to go to a specific file for processing.
 - **Secret Key:** This field is reserved for future use.
 - **Port:** This is the port that the AP will use to send records to the server. The server should be configured to listen for the billing records on that port.
10. Click **OK** to save the new settings.

XML Packet Format

The AP sends a string of XML commands to the specified billing servers according to the XML specification (see [XML Interface Specification](#)). The AP adds HTTP headers to the XML packets so that the billing servers receive the packets in HTTP-compliant XML format.

The XML string is in the following format:

AP to Server:

```

1 <AP RTMLOG_COMMAND="ADD_REC">
2   <REC_NUM> max 5 characters </REC_NUM>
3   <AP_ID> max 6 characters </AP_ID>
4   <PROPERTY_ID> max 64 characters </PROPERTY_ID>
5   <DATE> max 10 characters </DATE>
6   <TIME> max 8 characters </TIME>
7   <ROOM_NUM> max 20 characters </ROOM_NUM>
8   <AMOUNT> max 10 characters </AMOUNT>
9   <TRANS_TYPE> max 5 characters <TRANS_TYPE>
10  <SIGNATURE> max 16 characters </SIGNATURE>
11 </AP>
  
```

Sample format for each field:

1. REC_NUM: 00923 (numbers only, no alpha characters)
2. AP_ID: 4a672a
3. PROPERTY_ID: Any regular string
4. DATE: 04/18/2003 (mm/dd/yyyy)
5. TIME: 22:12:34 (24 hour format)
6. ROOM_NUM: Any regular string (not used)
7. AMOUNT: 234.34
8. TRANS_TYPE: Credit Card (CC)
9. SIGNATURE: Encrypted signature for authentication
- RESULT_VALUE: OK or ERROR
- IP: Standard IP address format

XML to AP:

The AP accepts a single line of XML text in the specified format (see [XML Interface Specification](#)). The XML string is a command sent by an external server to the AP. In this case, the acknowledgment received from the external server forms the command. The AP expects the acknowledgment in the following format:

```

<AP COMMAND="RTMLOG_ACK">
<ACK_VALUE>RESULT_VALUE</ACK_VALUE>
<IP_ADDR>AP's IP</IP_ADDR>
<ERROR_CODE>ERROR_CODE</ERROR_CODE>
</AP>
  
```

Public Space Parameters

Example of a Positive Acknowledgment:

```
<AP COMMAND="RMTLOG_ACK">
<ACK_VALUE>OK</ACK_VALUE>
<IP_ADDR>205.23.43.12</IP_ADDR>
<ERROR_CODE>1</ERROR_CODE>
</AP>
```

Example of a Negative Acknowledgment:

```
<AP COMMAND="RMTLOG_ACK">
<ACK_VALUE>ERROR</ACK_VALUE>
<IP_ADDR>205.23.43.12</IP_ADDR>
<ERROR_CODE>5</ERROR_CODE>
</AP>
```

Format for each field:

RESULT_VALUE: OK or ERROR

IP: standard IP format

ERROR_CODE: 1 for OK, or any other number for an error.

Logging

You can configure the AP-2500 to send system events and/or AAA events to network servers using the Syslog protocol. You can specify a single server to receive both types of messages or you can specify a different server for each message type.

General Syslog Information

- The Syslog message format is defined in RFC 3164 (see <http://www.rfc-editor.org/>).
- The AP transmits Syslog messages to the specified server(s) using the well-known UDP Syslog port (514).
- You need a Syslog server program running on a network computer to receive Syslog messages from the AP.
 - Kiwi Enterprises has a freeware Syslog Daemon for Windows operating systems. You can download the program at <http://www.kiwisyslog.com/>.
- Syslog Events are logged according to the level of detail specified by the administrator. Logging only urgent system messages will create a far smaller, more easily read log than a log of every event the system encounters. Determine which events to log by selecting a priority defined by the following scale:

Event	Priority	Description
LOG_EMERG	0	system is unusable
LOG_ALERT	1	action must be taken immediately
LOG_CRIT	2	critical conditions
LOG_ERR	3	error conditions
LOG_WARNING	4	warning conditions
LOG_NOTICE	5	normal but significant condition
LOG_INFO	6	informational
LOG_DEBUG	7	debug-level messages

Public Space Parameters

Configuration Instructions

Follow these steps to enable the AP's syslog features:

1. Login to the AP's Web browser interface.
2. Click **PublicSpace > Logging**.
3. Place a check mark in the **System Log** box to enable the logging of system message.
4. Place a check mark in the **AAA Log** box to enable the logging of AAA events.

⇒ NOTE

You can enable either or both of these log types.

5. Select a **System Log Number** (if you enabled System Log).
 - The default value is 2 (LOG_CRIT and higher).
 - You may want to set this to 7 so you receive all messages if this is the first time you are enabling this feature. If this generates too many messages you can always change the priority level at a later date.
6. Select an **AAA Log Number** (if you enabled AAA Log).
 - The default value is 3 (LOG_ERR and higher).
 - You may want to set this to 7 so you receive all messages if this is the first time you are enabling this feature. If this generates too many messages you can always change the priority level at a later date.

⇒ NOTE

The **Log Number** (between 0 and 7) corresponds to an event priority level. The AP will send event messages to the Syslog server that correspond to the selected priority and above. For example, if set to 6, the AP will transmit event messages labeled priority 0 to 6 to the Syslog server(s).

7. Enter the IP address of the server that will receive the System Log messages in the **System Log Server IP** field (if you enabled System Log).
8. Enter the IP address of the server that will receive the AAA Log messages in the **AAA Log Server IP** field (if you enabled AAA Log).

⇒ NOTE

The servers you specify must be running a Syslog program to properly log the messages. Also, you can send both message types to the same server, if necessary (although you may find it difficult to sort through a single log file that contains both types of messages).

9. Click **OK**.

Figure 5-15 Logging Screen

Public Space Parameters

Sample Logging Events

- [AAA Messages – Credit Card](#)
- [AAA Messages – Internal Web Server – User Name Login](#)
- [AAA Messages – RADIUS](#)
- [AAA Messages – XML](#)
- [Bill Mirror](#)
- [DHCP](#)
- [DNS](#)
- [Home Page Redirect](#)
- [Other AAA Messages](#)
- [Reboot Requests](#)

AAA Messages – Credit Card

Message	Meaning
USG_AAA: 4505 AAA_AuthProcess Credit_card:successful 00:50:04:29:37:56 Exp_time:24 hrs 0 min	Successful Credit Card purchase
USG_AAA: 4503 AAA_AuthProcess_Authentication Unsuccessful__Not_approved_by_CC 00:50:04:29:37:56	Failed Credit Card transaction

AAA Messages – Internal Web Server – User Name Login

Message	Meaning
USG_AAA: 4509 AAA_AuthProcess Updated_successfully 00:50:04:29:37:56 x	Successful Login
USG_AAA: 4100 AAA_lookup Time_expired 00:50:04:29:37:56 bytes:98769	User's time has expired
USG_AAA: 4006 AAA_Interface Removed_by_administrator 00:50:04:29:37:56	User's profile has been deleted by the administrator

AAA Messages – RADIUS

Message	Meaning
USG_AAA: 4301 Expired_time Expired_time_entry_will_be_reused 00:50:04:29:37:56 bytes:25485	User has been removed due to Session Timeout
USG_AAA: 4303 update_Timer_Timeout expired_time_entry_reused 00:50:04:29:37:56 Bytes:14698	User has been removed due to Idle Timeout
USG_AAA: 4904 AAA_Radius Old_radius_resp	This occurs if the user has already tried to login before.
USG_GOA: Radius server should have timed out.	This occurs when the AP would have expected the RADIUS client to report that the RADIUS access-request timed out. This can occur if the RADIUS client is very busy processing other requests.

Public Space Parameters

AAA Messages – XML

Message	Meaning
USG_AAA: 4007 AAA_Interface added_by_administrator 00:50:04:29:37:56 Exp_time:24 hrs 0 min	User added
USG_AAA: 4800 AAA_XML Memory_updated__State_valid 00:50:04:29:37:56	Update Cache executed
USG_AAA: 4006 AAA_Interface Removed_by_administrator a	User Delete issued for user a

Bill Mirror

Message	Meaning
RMTLOG: rmtlogXmlTcpSend: Connect error	Bill Mirror enabled, but the server does not respond
RMTLOG: rmtlogXmlTcpSend: transmission Ok	Bill Mirror enabled, and response received from server

DHCP

Message	Meaning
DHCP: dhcpStart: dst port (68) not DHCP server port	This indicates that there is another DHCP server on the subscriber side of the AP.
DHCP: dhcpStart: Invalid DHCP options packet	This means that the client sent an invalid DHCP cookie. If this is seen, it could mean data errors in network or a non-compliant DHCP client.
DHCP: dhcpStart: invalid IP header	This could be caused by a non-compliant DHCP client or data errors in the network.
DHCP: garbage_collect: dangling bind structure bindptr->data = 0x3efdb14 cid = 0x000000000000 IP = 61.193.248.17 -- I	The AP code attempts to clean up DHCP bindings that have been turned off and a subscriber in the subscriber table appears with the same IP address.
DHCP: icmp_check: BAD... conflict: Req: MAC 00-00-0E-FE-87-09; In SubTable: IP 219.103.171.66 MAC 00-05-02-CB-58-23	This happens if the DHCP lease the AP wants to hand out already exists in the Subscriber table. If it does, then the AP will skip this lease and go on to the next one.
DHCP: turnoff_bind: binding passed is NULL!	This can happen if the code tries to turn off a resource because there's someone on the subscriber side that is already using that address. In this case, if the resource does not have a corresponding binding, this syslog will result.
DHCP: Warning: DHCPDISCOVER - No available addresses in the pool.	There are no more available leases in the DHCP server lease pool and a DHCP request has been received.
WARNING DHCP: read_bind_db: can't find resource usg13d733121 in nmhashtable	This occurs if the DHCP Lease pool settings have been changed in the AP and the lease is not part of the new pool.
usgDHCPInit: server and relay are OFF	DHCP Services have been disabled on the AP.

Public Space Parameters

DNS

Message	Meaning
USG_DNS:ndxDNSRedirectionTable::processFromNetwork(): could not get subid	This syslog suggests that the AP could not get the subscriber associated with a particular DNS redirection request.
USG_DNS:ndxDNSRedirectionTable::processFromSubscriber(): dnsIsQueryA() failed	The AP has received a DNS packet that was not a valid DNS query and is not processed.
USG_DNS: ndxService::processKnownNames(): dnsIsQueryA() failed	The AP has received a valid DNS query, which failed.
ndxDNSRedirectionTable::processFromNetwork(): duplicate reply or reply without request	The AP has received a DNS reply from the network side but does not have a matching request.
USG_DNS: dnsRedirectFromSub(): GetDNSServerIP failed	This occurs when redirecting the DNS packet and the DNS server cannot be found.
USG_DNS:ndxDNSRedirectionTable::dnsSubPktForRedirection Table(): GetSubId() failed	This syslog suggests that the AP could not get the subscriber associated with a particular DNS redirection request.
USG_DNS: ndxDNSService::FromSubscriber(): Unable to determine if redirection is needed	The AP was unable to redirect the DNS request because the packet had the wrong packet info type.

Home Page Redirect

Message	Meaning
USG_HRS: 3009 HRS_Object _returned_by_HRS_GetRequestMethod	The HTTP request method is invalid.
USG_HRS: 3010 HRS_Object received_bad_URL	The HTTP request was null, empty, or incorrectly formed.
3014 HRS_Object ERROR_writing_to_the_socket	The AP could not write to socket so the user did not received an appropriate response to their http request.
USG_HPR: 3017 HPR_Functionality received_a_request_of_unknown_type	The HTTP request method is not GET, POST or HEAD. The AP cannot handle this type of request so it is ignored.
USG_HRS: 3025 HRS_Object Socket ReadERROR: sFD 17 read bytes -1, errno=54	This occurs if the connection is reset by the peer machine and the AP cannot read the http request.
USG_HPR: 3026 HPR_Functionality Socket_timeout	This occurs when the AP does not receive a complete request from the subscriber.

Public Space Parameters

Other AAA Messages

Message	Meaning
AAA: 4121 AAA_lookup Tried to add blacklisted IP 210.155.227.244 or MAC 00:50:E8:00:07:99	Attempting to add a blacklisted IP to subscriber table. IP is 'blacklisted' when its one of the IPs known to not belong to a subscriber (i.e. Network/Subscriber IP of the AP, etc.).
USG_AAA: 4006 AAA_Interface Removed_by_administrator 00:00:78:02:1D:70 USG_AAA: 4006 AAA_Interface Removed_by_administrator aforum	Subscriber's profile was removed by an administrator.
USG_AAA: 4007 AAA_Interface Added_by_administrator ahughes Exp_time:Unlimited	Subscriber's profile was added to the database with a user name.
USG_AAA: 4009 AAA_Interface Updated_by_administrator 00:03:47:F0:8F:72 Exp_time:Unlimited	Subscriber's profile was updated by an administrator
USG_AAA: 4013 AAA_Interface Cache_entry_removed 00:03:47:F0:8F:72 bytes:165304	A Pending or RADIUS user's profile has been removed from the Current Subscribers list.
USG_AAA: 4102 AAA_lookup Time_expired 00:00:39:05:53:3A	Pending user has been removed from the Current Subscribers list by the cleanup routine.
USG_AAA: 4104 AAA_lookup Memory_updated__State_valid 00:00:21:DB:FD:D3	A Pending user has been changed to Valid because his MAC address already exists in the internal database of the AP.
USG_AAA: 4106 AAA_lookup Added_in_memory_table__Pending 00:00:4C:3B:3B:22	A subscriber appears on the AP and has not yet authenticated. This will appear only if AAA is enabled.
USG_AAA: 4115 AAA_lookup Location_changed 00:00:39:05:53:3A bytes:0	This occurs if a subscriber has changed from one VLAN to another.
USG_AAA: 4119 AAA_lookup Disconnected 00:90:CC:00:41:40 bytes:29981231	A subscriber has been removed from the Current Subscribers list due to inactivity. The subscriber's profile has not been deleted in this case.

Reboot Requests

Message	Meaning
CLI_TN: 0254 Requesting reboot	Reboot requested via Telnet session
WWS: 0254 Requesting reboot	Reboot requested via Web Interface
CLI_SR: 0254 Requesting reboot	Reboot requested via Serial connection

URL Filtering

The AP-2500 can restrict access to specified web sites based on URLs. URL filtering will block access to these list of sites and/or domains. You can restrict access to specific Web sites based on IP address, DNS name (for example *www.yahoo.com*) or DNS Domain name (for example, **.yahoo.com*, meaning all sites under the yahoo.com hierarchy, such as *finance.yahoo.com*).

There is one filtering table for IP addresses and a second for DNS names. Each table can hold up to 50 entries.

Figure 5-16 URL Filter Screen

URL Filtering by DNS Names

1. Login to the AP's Web browser interface.
2. Click **PublicSpace** > **URLFilter**.
3. Place a check mark in the **Enable URL Filtering** box.
4. Click the **Add** button above the **URL Filtering by DNS Names** heading.
5. Enter the DNS name to filter in the **URL** field and click **OK**.
 - Enter "www.myhotspot.com" to block access to that specific web address.
 - Enter "*.myhotspot.com" to block access to all sites associated with the specified DNS name.
6. Enter a second DNS name to filter (if applicable) and click **OK**. Continue until you have entered all of the names you want to filter.
7. Click the back arrow button to return to the previous screen.
8. Reboot the AP.

If you later want to edit or delete an entry, click the **Edit** button.

- To delete an entry, change the **Status** to **Destroy**.
- Only Active and Destroy are valid options within the **Status** field when using the Web browser interface.

Public Space Parameters

URL Filtering by IP Address

1. Login to the AP's Web browser interface.
2. Click **PublicSpace > URLFilter**.
3. Place a check mark in the **Enable URL Filtering** box.
4. Click the **Add** button above the **URL Filtering by IP Address** heading.
5. Enter the IP address to block in the **IP Address** field and click **OK**.
6. Enter a second IP address to block (if applicable) and click **OK**. Continue until you have entered all of the IP address that you want to block.
7. Click the back arrow button to return to the previous screen.
8. Reboot the AP.

If you later want to edit or delete an entry, click the **Edit** button.

- To delete an entry, change the **Status** to **Destroy**.
- Only Active and Destroy are valid options within the **Status** field when using the Web browser interface.

Information and Control Console (ICC)

The AP-2500 supports an optional Information and Control Console (ICC), which can be presented to subscribers in the form of a pop-up window when new web browsers are opened. This allows easy modifications to billing plans, redirections to predetermined web sites, and options for displaying advertising banners.

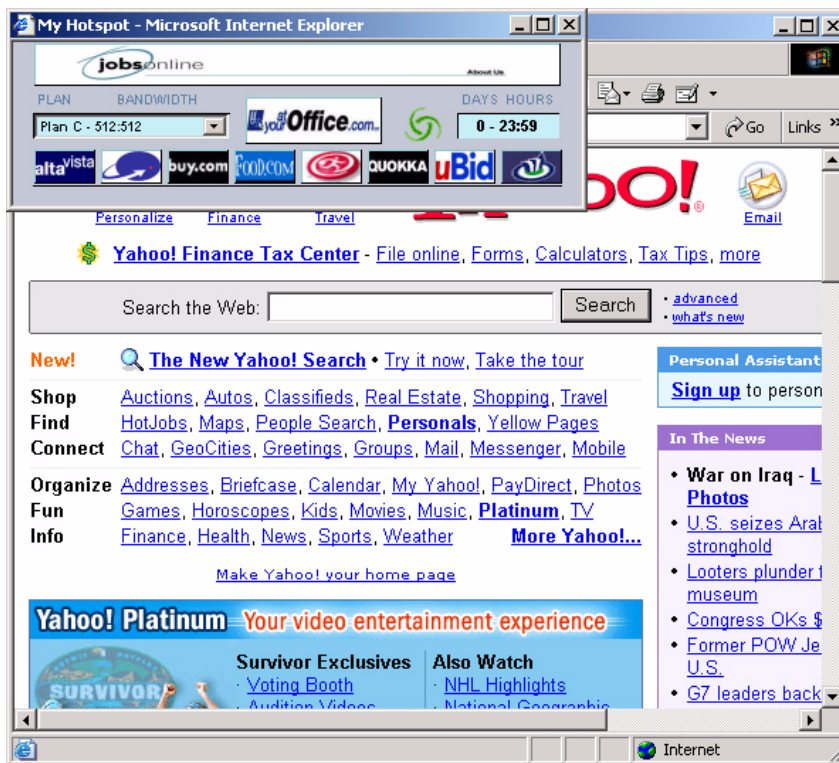


Figure 5-17 Information and Control Console (ICC)

The ICC is disabled by default. You can enable this feature and customize its content from the **PublicSpace > ICC** screen.

Public Space Parameters

ICC Appearance

The ICC screen contains the following items:

- Title Bar
 - Appears at the top of the screen near the Web browser name.
- Ad Banner
 - You can specify up to 5 different banners that share this space.
- ISP Button
 - Appears in the center of the ICC.
 - You can customize this button to display your own logo.
- 8 Ad Buttons
 - The bottom row of buttons of the ICC.
- Text Bar
 - Located at the bottom of the ICC.
 - It displays custom text when the cursor is rolled over a button or banner.
- Dynamic Billing Plan Selection field
 - This option does not appear for all customers (see below).
 - Subscribers can select a new billing plan from the drop-down menu.
- Count-down Timer
 - This option does not appear for all customers (see below).
 - This field displays the subscriber's remaining access time.
 - This field shares the same space as the Logout button.
- Logout Button
 - This option appears for all customers authenticated by a RADIUS server (if using Internal authentication with RADIUS).
 - This field shares the same space as the Count-down Timer field.

The appearance of the ICC will vary depending on the subscriber's access method. For example, if a subscriber has been authenticated by a RADIUS server, a **Logout** button will appear on the ICC. If a subscriber purchased access time with a credit card, a count-down timer will appear on the ICC.

The following images illustrate the ICC appearance for each access method. Note that all of these images use the default graphics.

Free Access/Manual Configuration

If you offer a free billing plan or if you manually added a user to the Authorized Subscribers Table, the ICC does not display the Dynamic Billing Plan Selection field, the Count-down Timer, or the Logout button:



Figure 5-18 ICC Screen

Credit Card Purchase

If a subscriber purchased access time by credit card, the ICC includes the Count-down Timer and the Dynamic Billing Plan Selection field:

Public Space Parameters



Figure 5-19 ICC Screen -- Credit Card

Authenticated by RADIUS

If a subscriber has been authenticated by a RADIUS server (if using Internal authentication with RADIUS), the ICC includes a Logout button so customers can end their session. The ICC also displays the subscriber's current billing plan in the Dynamic Billing Plan Selection field. Note that the subscriber will not be able to change the billing plan unless you enable the Nomadix-IP-Upsell RADIUS Vendor Specific Attribute (VSA). See [Install and Configure RADIUS](#) and [RADIUS Messages and RADIUS Attributes](#) for details.



Figure 5-20 ICC Screen -- RADIUS

Customizing the ICC

You can customize the buttons, banners, and ISP logo button that appear on the ICC. All of the image files for the ICC are stored in the AP in a ZIP file named **images.zip**. Follow these steps:

1. Determine the design of the ICC and decide which buttons you want to customize.
2. Obtain or design the images that will appear on the ICC.
 - You can customize:
 - Up to 5 Banners: 373 pixels (width) x 32 pixels (height)
 - One ISP Button: 98 pixels (width) x 26 pixels (height)
 - Up to 8 Small Buttons: 45 pixels (width) x 26 pixels (height)
 - The images should conform to the size restrictions listed above and be in JPG or GIF format.
 - Assign names to the files so they can be easily identified and remembered.
3. Create a ZIP file named **images.zip** that contains all of the ICC image files.
 - To review the image files currently loaded with the ICC, see the *images.zip* file in the CD's *Docs/samples/* folder.
 - Alternatively, you can upload the current *images.zip* file from the AP to your TFTP server using the [Upload](#) command. The File Name is **images.zip** and the File Type is **Generic**.
4. Copy the new *images.zip* to your TFTP server's root directory.
5. Login to the AP's Web browser interface.
6. Click **Commands > Download**.
7. Use the [Download](#) command to download the new *images.zip* to the AP.
 - The File Name is **images.zip** and the File Type is **Generic**.
 - This will overwrite the existing *images.zip* file.
8. Click **PublicSpace > ICC > Basic**.

Public Space Parameters

ICC Setup

Enable ICC ☒

Title

ICC on subscriber session close ☒ Redisplay ☐ Logout

	Name/Text	Target URL	Image Name
ISP Logo Button	Atyouroffice.com	http://www.atyouroffice.co	AtyourofficeBigbutton.jpg
Button 2	Altavista	http://www.altavista.com	AltavistaButton.jpg
Button 3	Travelscape	http://travelscape.com	TravelscapeButton.jpg
Button 4	BUY.COM	http://www.buy.com	BuyButton.jpg
Button 5	Food.com - order on line	http://www.food.com	FoodButton.jpg
Button 6	STORERUNNER.COM	http://www.storerunner.co	StorerunnerButton.jpg
Button 7	The Quokka Sports Netwo	http://www.quokka.com	QuokkaButton.jpg
Button 8	UBID - where you set the	http://www.ubid.com	UbidButton.jpg
Button 9	Make the most of your cit	http://www.citysearch.com	CitysearchButton.jpg

OK Cancel

Figure 5-21 ICC Setup Screen

9. Place a check mark in the **Enable ICC** box.
10. Enter the **Title** for the ICC.
 - This is the name that appears at the top of the ICC next to the Web browser name.
11. Configure the **ICC on subscriber session close** option.
 - When set to **Redisplay**, the ICC reappears approximately 5 minutes after a subscriber closes it but only in response to a new URL request from the user.
 - For example, if a user closes the ICC and remains on the same Web page for more than 5 minutes, the ICC will not reappear. However, it will reappear the next time the user tries to access a new Web page.
 - When set to **Logout**, the subscriber is automatically logged out when he/she closes the ICC.
 - This setting is only applicable if your subscribers are authenticated by a RADIUS server.
 - This setting is not generally recommended. If you do select this option, you should notify your subscribers of the consequences of closing the ICC.

Public Space Parameters

12. Configure the **ISP Logo Button** settings.
 - Enter the Name or Title of the ISP Button in the ISP Logo Button's **Name/Text** field.
 - This is the text that will appear in the text bar at the bottom of the ICC when a subscriber rolls over the icon with his/her mouse cursor.
 - In the **Target URL** field, enter the Web address to which a subscriber will be redirected upon clicking the ISP Logo Button.
 - Enter the name of the ISP Logo button image file in the **Image Name** field.
 - This name must match the logo file you downloaded to the AP in the **images.zip** file.
13. Configure the settings for **Button 2** through **Button 9**, as necessary.
 - These buttons correspond to the lower row of buttons in the ICC.
 - Enter the Name or Title of the button in the appropriate **Name/Text** field.
 - This is the text that will appear in the text bar at the bottom of the ICC when a subscriber rolls over the icon with his/her mouse cursor.
 - In the **Target URL** field, enter the Web address to which a subscriber will be redirected upon clicking the specified button.
 - Enter the name of the button image file in the **Image Name** field.
 - This name must match the image file you downloaded to the AP in the **images.zip** file.
14. Click **OK**.
15. Click the **Banner1** tab.

Figure 5-22 Assigning Banners Screen

16. Configure the settings for Banner 1.
 - Set the **Banner Name**.
 - This is the text that will appear in the text bar at the bottom of the ICC when a subscriber rolls over the icon with his/her mouse cursor.
 - In the **Banner URL** field, enter the Web address to which a subscriber will be redirected upon clicking the banner.
 - Set the **Banner Duration**, in seconds (from 1 to 9999; 0 disables the banner).
 - This is how long the banner will appear on the ICC before moving on to the next banner.
 - The Web browser interface labels this parameter in **Mins** but it should be **Seconds**. By default, the banners change every 6 seconds.

Public Space Parameters

- Configure the optional banner **Start Time** and **Stop Time**.
 - The Start Time is in **hh:mm AM/PM** format and determines when the banner will be displayed on the ICC. After the start time elapses, the banner appears in the ICC for the specified Banner Duration along with the other enabled banners. The banner is disabled before the start time.
 - The Stop Time is in **hh:mm AM/PM** format and determines when the banner stops appearing on the ICC.
 - If these fields are left blank, the specified banner always appears in the ICC for the specified Banner Duration (assuming it is not 0).



NOTE

Banner Start and Stop Times are based on the subscriber's clock time, not the AP's. If you're testing this feature, logout the subscriber and login again to refresh the ICC.

- Click **OK**.
17. Click the appropriate **Banner** tabs and configure the other banners using the procedure described above, if necessary.
 18. Reboot the AP.

Potential End User Issues

If you plan to enable ICC for your subscribers, you should be aware of several potential issues that your customers may encounter:

- **No Support for Windows CE:** Windows CE devices do not currently support Java and, therefore, do not currently support the ICC. If you have enabled ICC and a subscriber is using a PDA running Windows CE, the PDA's browser will lock up while trying to load the ICC. Do not enable ICC if you expect your subscribers to be using PDAs to connect to the AP.
- **Internet Explorer Java Support:** Due to recent changes in the relationship between Microsoft and Sun Microsystems, Windows customers who do not already have a version of Java Virtual Machine installed may encounter a problem viewing the ICC. By default, Windows Internet Explorer attempts to download Microsoft's Java Virtual Machine plug-in if a Java Virtual Machine is not already installed. However, Microsoft no longer provides this download so your customer's browser may hang. The solution is to download Java Virtual Machine from Sun Microsystems (see <http://java.sun.com/getjava/>) and/or update to the latest version of Microsoft Windows Explorer.
- **ICC and Cached Pages:** The ICC appears after successful login or re-login only when a customer accesses a new Web page. The ICC may not appear if the customer requests a Web page that is already in the browser's cache. The solution is to have the customer access a new Web page and the ICC will appear.
- **RADIUS Logout Button Does Not Work With Sun's Java Virtual Machine:** If the subscriber has a Java virtual machine installed, then the ICC will use this Java machine (even if Internet Explorer also has Microsoft's Java program installed). In this case, if the customer clicks the **Logout** button in the ICC, he is not logged out and the session remains active until the idle timer expires or the subscriber uses the <http://1.1.1.1/> URL to logout.
- **Logout Button Does Not Work Following a Roam:** A RADIUS user who clicks the **Logout** button will not be logged out following a roam from one AP-2500 to another. The user will need to browse new pages to bring up the login screen for the new AP and re-login when prompted. See [Limitations on Roaming](#) for more information.

SMTP Redirection

This tab allows you to configure the AP-2500 to pass subscriber's e-mail through a dedicated Simple Mail Transfer Protocol (SMTP) server independent of a subscriber's (misconfigured and/or properly configured) computer settings. Most SMTP servers only transmit e-mail messages that originate from local traffic to prevent illegal use of a mail server by spammers, hackers, and other unauthorized individuals. Therefore, most of your subscribers will be unable to send e-mail messages unless you enable SMTP Redirection.

When this feature is enabled, it is transparent to the user. All outgoing mail traffic is redirected to the SMTP server you specify in the **SMTP Server IP** field (this field is based on IP address and not DNS name). This will allow subscribers to send e-mails without changing any of the server settings in their e-mail program. Typically, this will be your local mail server (if you have one) or your ISP's mail server.

Public Space Parameters

Follow these steps to enable SMTP Redirection:

1. Login to the AP's Web browser interface.
2. Click **PublicSpace** > **SMTP**.
3. If you want all outgoing mail traffic redirected to the specified server, enable both the **Misconfigured** and **Properly Configured** options. If you want properly configured subscribers to send mail without being redirected, enable only the **Misconfigured** option.
 - **Misconfigured** refers to subscribers whose e-mail settings are incompatible with the AP-2500's Internet settings (in other words, these e-mail settings may work on the subscriber's home or office network but they won't work in the hotspot).
 - **Properly Configured** refers to subscribers whose e-mail settings should work on the hotspot network so you do not necessarily need to redirect these messages to your own server.



NOTE

In general, Proxim recommends that you enable both options. Also, you should never enable **Properly Configured** and disable **Misconfigured** (this combination defeats the purpose of SMTP Redirection).

4. Enter the IP address of the SMTP server to which outgoing e-mails will be redirected in the **SMTP Server IP Address** field.
5. Click **OK**.

Figure 5-23 SMTP Screen

Passthrough Addresses

This tab provides a method for DNS Names, IP Addresses, and an AAA port to “passthrough” the AP-2500 and access pre-determined services (for example, a portal page) without authentication. This feature also allows you to create a “walled garden” of free content that you can provide to your customers. Typically, the walled garden content would appear on your portal page or custom login page. See [Portal Page](#) for more information.

The following DNS names or addresses must appear in a Passthrough table for the related feature to work properly:

- Portal Page server address
- Credit Card server address
- External Web Server address (if using External authentication)
- The Domain Names or IP addresses for walled garden content

Public Space Parameters

The DNS and IP Address tables can hold up to 50 entries each. The AAA port option supports only passthrough port.

- [Passthrough DNS Table](#)
- [Passthrough IP Table](#)
- [Passthrough AAA Port](#)

The screenshot shows the Proxim Web browser interface. On the left is a sidebar with buttons: Status, Configure, Monitor, Commands, **PublicSpace**, Subscriber, Help, and Exit. The main content area has tabs: HPR, AAA, Logging, URLFilter, ICC, SMTP, **Passthrough**, and Bandwidth Mgmt. Under the **Passthrough** tab, there are sub-tabs: **IP/DNS** and AAA Port. The **IP/DNS** sub-tab is active and contains the following text:

This tab is used to configure IP/DNS passthrough settings. This feature allows users to "pass through" and access predetermined services without authentication.

Note: DNS name must not contain port, protocol or path information

Changes to these parameters require access point reboot in order to take effect.

Enable Passthrough Address ☒

Passthrough DNS Table

Buttons: Add, Edit

DNS Names	Status
tvguide.com	Active
weather.com	Active
coffeeuniverse.com	Active

Passthrough IP Table

Buttons: Add, Edit

IP Address	Status
206.253.210.201	Active
192.168.0.101	Active

Figure 5-24 IP/DNS Passthrough Table

Passthrough DNS Table

1. Login to the AP's Web browser interface.
2. Click **PublicSpace** > **Passthrough** > **IP/DNS**.
3. Place a check mark in the **Enable Passthrough Address** box.
4. Click the **Add** button below the **Passthrough DNS Table** heading.
5. Enter the DNS name to filter in the **DNS Name** field and click **OK**.
 - Enter "www.myhotspot.com" to allow access to a specific web address.
 - Enter "*.myhotspot.com" to allow access to all sites associated with the specified DNS name.
 - Do not include port, protocol, or path information when enter DNS names.
6. Enter a second DNS name (if applicable) and click **OK**. Continue until you have entered all of the names you want to add to the table.
7. Click the back arrow button to return to the previous screen.
8. Reboot the AP.

If you later want to edit or delete an entry, click the **Edit** button.

- To delete an entry, change the **Status** to **Destroy**.
- Only Active and Destroy are valid options within the **Status** field when using the Web browser interface.

Public Space Parameters

Passthrough IP Table

1. Login to the AP's Web browser interface.
2. Click **PublicSpace > Passthrough > IP/DNS**.
3. Place a check mark in the **Enable Passthrough Address** box.
4. Click the **Add** button below the **Passthrough IP Table** heading.
5. Enter the IP address to passthrough in the **IP Address** field and click **OK**.
6. Enter a second IP address (if applicable) and click **OK**. Continue until you have entered all of the IP addresses that you want to passthrough.
7. Click the back arrow button to return to the previous screen.
8. Reboot the AP.

If you later want to edit or delete an entry, click the **Edit** button.

- To delete an entry, change the **Status** to **Destroy**.
- Only Active and Destroy are valid options within the **Status** field when using the Web browser interface.

Passthrough AAA Port

The DNS and IP Passthrough tables only apply to WWW-HTTP traffic on port 80. You can enable passthrough traffic on a second port if necessary for AAA purposes.

For example, if you have a secure custom login page on an External Web Server, you can enable HTTPS traffic on port 443 so that unauthenticated users can access the page. This will allow the AP to pass HTTPS traffic for unauthenticated users. This is in addition to the standard port 80 traffic that the AP passes based on the IP and DNS Passthrough Tables.

Follow these steps to enable a Passthrough AAA Port:

1. Login to the AP's Web browser interface.
2. Click **PublicSpace > Passthrough > AAA Port**.
3. Place a check mark in the **Enable Passthrough Port** box.
4. Enter the AAA port in the **Passthrough Port Number** field.
 - Do not enter port 80, 2111, 1111, or 1112.
5. Click **OK**.
6. Reboot the AP.

Bandwidth Management

The AP-2500 can manage the bandwidth for subscribers, defined in Kbps, for both upstream and downstream data transmissions. With the ICC feature enabled, subscribers can increase or decrease their own bandwidth dynamically (by the minute, or on an hourly, daily, weekly, or monthly basis), and also adjust the pricing plan for their service.

If you plan to limit subscriber bandwidth or offer multiple access plans based on bandwidth speeds, click the **Bandwidth Mgmt** tab to notify the AP of its bandwidth settings.

These parameters correspond to the AP's connection to the Ethernet and the Internet. Based on these settings, the AP determines the speed of its Internet connection. The AP uses this information when making bandwidth allocations to subscribers. Keep in mind the following points:

- Do not set uplink or downlink speed to 0; this will disable access to the unit over the Ethernet.
- The upper limit for uplink or downlink speed is 100,000 Kbps (100 Mbps). This is the maximum speed at which the AP can connect to the Ethernet network. In reality, the uplink and downlink speeds will depend upon the speed of your hotspot's Internet connection (for example, T1 or DSL) and the speed of the wireless cards installed in the AP.
- By default, Bandwidth Management is enabled and uplink and downlink speeds are set to 1500 Kbps.

Follow these steps to enable Bandwidth Management:

1. Login to the AP's Web browser interface.
2. Click **PublicSpace > Bandwidth Mgmt**.
3. Place a check mark in the **Enable Bandwidth Management** box.

Public Space Parameters

4. Enter the speed of the connection between the AP and the Ethernet network in the **Bandwidth uplink (to network) speed** field (in Kbps).
5. Enter the speed of the connection between the AP and the wireless clients in the **Bandwidth downlink (to subscribers) speed** field (in Kbps).
6. Click **OK**.
7. Reboot the AP.

The screenshot displays the Proxim Bandwidth Management configuration interface. On the left is a vertical sidebar with buttons: Status, Configure, Monitor, Commands, PublicSpace (highlighted in orange), Subscriber, Help, and Exit. The main window has a top navigation bar with tabs: HPR, AAA, Logging, URLFilter, ICC, SMTP, Passthrough, and Bandwidth Mgmt (highlighted in orange). Below the tabs, a message states: "This tab is used to limit the bandwidth for subscribers for both upstream and downstream data transmissions." followed by a note: "Note: Reboot required for this change to take effect." The configuration area includes a checkbox for "Enable Bandwidth Management" which is checked. Below this are two input fields: "Bandwidth uplink (to network) speed" and "Bandwidth downlink (to subscribers) speed", both containing the value "1500" and followed by "Kbps". At the bottom of the main area are "OK" and "Cancel" buttons.

Figure 5-25 Bandwidth Management Screen

Billing Options for Subscribers

The Web browser interface's **Subscriber** button links to three screens that allow you to configure Subscriber billing plans (**Billing** tab), login and error messages (**Messages** tab), and the Authorized Subscribers database (**Authorized** tab).

NOTE

The Billing and Messages options are used in conjunction with the Internal Web Server. You do not need to configure these options if using an External Web Server.

The **Internal Billing Options** screen defines the billing plans that you want to offer to your subscribers.

Billing Messages Authorized

Options Mirroring Plan 0 Plan 1 Plan 2 Plan 3 Plan 4 Plan 5

This tab is used to define various billing options for use with Internal Web Server based on messages displayed, billing schemes (units of access) and zero billing options (free access).

Internal Billing Options

Introduction Message: The following plans are available:
Offer Message: How much access would you like to purchase?
Policy Message: You will be billed per hour based upon which plan you select

Minimum Units of Access To Purchase: 1

Units of Access:
☐ Minute
☒ Hour
☐ Day
☐ Week
☐ Month

Free Billing Options

Default Free Access Time: 7 Mins
Maximum Lifetime: 180 Mins

OK Cancel

Figure 5-26 Billing Options Screen

Follow these steps to configure the billing plans:

1. Login to the AP's Web browser interface.
2. Click **Subscriber > Billing > Options**.
3. Configure the messages that will appear on the login screen where new users select a billing plan, as shown in the following example (without the logo image).

Public Space Parameters

Please Choose from the following plans.

Plan Name	per Day	Features
<input type="radio"/> Plan A	\$8.95	256K downstream, 128K upstream
<input checked="" type="radio"/> Plan B	\$9.95	512K downstream, 256K upstream

How many days of Internet access would you like to purchase?

Contact your service provider with questions.

Please enter a new user ID and password:

Choose a User ID (optional)

Choose a Password (optional)

Retype the Password (if entered above)

Please contact your Network Administrator in case of problems.

Figure 5-27 Default New User Screen that Appears to Subscribers

- Edit the **Introduction Message**.
 - The default Introduction Message is “Please Choose from the following plans.”
- Edit the **Offer Message**.
 - The default Offer Message is “How many days of Internet access would you like to purchase?”
- Edit **Policy Message**.
 - The default Policy Message is “Contact your service provider with questions.”



NOTE

See [Subscriber Messages](#) for information on how to customize the text that appears on the other login pages presented to customers.

4. In the **Minimum Units of Access to Purchase** field, define the minimum units of access that subscribers must purchase.
5. Select a **Units of Access (Minute, Hour, Day, Week, or Month)** for your subscribers.



NOTE

You must use the same Unit of Access for all of your billing plans.

6. If you plan to offer a free billing plan (see [Creating a Free Billing Plan](#)), configure the **Free Billing Options**.
 - The **Default Free Access Time** specifies (in days) how long a customer will have uninterrupted free Internet access.
 - The **Maximum Lifetime** specifies (in days) the maximum amount of time a customer can use the free billing plan.
 - The Web browser interface labels this parameter in **Mins** but it should be **Days**.
 - For example, if you set **Default Free Access Time** to 1 day and **Maximum Lifetime** to 2 days, here is how the customer interacts with the AP:
 - Customer enters hotspot and is prompted to select a billing plan.
 - Customer selects free billing plan.
 - Customer has free access for one day.
 - After one day, the customer is prompted again by the **New User** screen to select a billing plan.
 - If the customer again selects the free plan, he will have free access for one more day (since the Maximum Lifetime for free access is set to 2 days).

Public Space Parameters

7. Click **OK**.
8. Click the **Plan 0** tab.
9. Configure the settings for billing plan 0.
 - Place a check mark in the **Enable Plan** box to make the plan active. It will appear as an option in the **New User** screen presented to subscribers.
 - Enter a name for the plan in the **Plan Label** field.
 - Enter a description for this billing option in the **Description of Service** field (140 characters maximum).
 - Define the pricing schemes for this billing plan (**Rate Per Minute**, **Rate Per Hour**, **Rate Per Day**, **Rate Per Week**, and **Rate Per Month**).
 - The AP will only use the pricing scheme that corresponds to the **Units of Access** you selected in the **Billing > Options** screen.
 - Define the **Upstream Bandwidth** and **Downstream Bandwidth** range for this billing plan.
 - Define the **DHCP Pool**: **Private** or **Public**.
 - If you want to use IP Upsell, be sure to configure at least plan to use Public IP address. See [IP Upsell](#).
 - Click **OK**.

The screenshot displays the 'Subscriber Billing Plans Screen' within a web-based management interface. On the left is a sidebar with buttons: Status, Configure, Monitor, Commands, PublicSpace, **Subscriber**, Help, and Exit. The main content area has tabs for 'Billing', 'Messages', and 'Authorized'. Under the 'Billing' tab, there are sub-tabs for 'Options', 'Mirroring', and 'Plan 0' (the active tab). Below these, a message states 'This tab is used to define a billing plan.' The form for 'Subscriber Billing Plan 0' includes the following fields and values:

Enable Plan	<input checked="" type="checkbox"/>
Plan Label	Plan A
Description of Service	256Kbps downstream, 128Kbps upstream
Rate Per Minute	2.00
Rate Per Hour	4.00
Rate Per Day	8.95
Rate Per Week	15.00
Rate Per Month	40.00
Up Stream Bandwidth	256
Down Stream Bandwidth	256
DHCP Pool	Private <input checked="" type="radio"/> Public <input type="radio"/>

At the bottom of the form are 'OK' and 'Cancel' buttons.

Figure 5-28 Subscriber Billing Plans Screen

10. Configure the other billing plans that you want to offer.
 - You can configure up to six different billing plans.
11. Reboot the AP.

Public Space Parameters

Creating a Free Billing Plan

Under some circumstances you may want to offer free Internet access to your subscribers. For example, you might offer a low bandwidth connection for free but charge for faster connections.

Follow these steps to make one of your six billing plans a free billing plan:

1. Login to the AP's Web browser interface.
2. Click **Subscriber > Billing > Plan x** (select a Plan number between 0 and 5).
3. Place a check mark in the **Enable Plan** box to make the plan active.
4. Enter a name for the plan in the **Plan Label** field.
5. Enter a description for this billing option in the **Description of Service** field (140 characters maximum).
6. Set all **Rates** to **0.00**.
7. Define the **Upstream Bandwidth** and **Downstream Bandwidth** range for this free plan.
8. Define the **DHCP Pool: Private** or **Public**. (Typically, a free plan is a private address pool).
9. Click **OK**.

The screenshot displays the 'Subscriber Billing Plan 5' configuration window. The 'Enable Plan' checkbox is checked. The 'Plan Label' is 'Free Access' and the 'Description of Service' is '56K downstream, 28K upstream'. All rate fields (Per Minute, Hour, Day, Week, Month) are set to 0.00. The 'Up Stream Bandwidth' is 28 and the 'Down Stream Bandwidth' is 56. The 'DHCP Pool' is set to 'Private'.

Figure 5-29 Configuring a Free Plan

Once configured, the free plan becomes an option in the **New User** screen presented to customers during login, as shown in the following example.

Public Space Parameters

Figure 5-30 Subscribers Can Select a Plan that Offers Free Internet Access

Subscriber Messages

The Web browser interface's **Subscriber** button links to three screens that allow you to configure Subscriber billing plans (**Billing** tab), login and error messages (**Messages** tab), and the Authorized Subscribers database (**Authorized** tab).

⇒ NOTE

The Billing and Messages options are used in conjunction with the Internal Web Server. You do not need to configure these options if using an External Web Server.

The **Subscriber Messages** screens let you customize the look and content of the AP's internal login screens that are presented to subscribers.

Follow these steps to customize the text and images that appear on AP's internal Web pages:

⇒ NOTE

See [Billing Options for Subscribers](#) for information on how to define billing plans and customize the text that appears on the **New User** screen presented to new customers.

1. Login to the AP's Web browser interface.
2. Click **Subscriber > Messages > Login Msgs**.

Public Space Parameters

The screenshot shows the Proxim configuration interface. On the left is a sidebar with buttons: Status, Configure, Monitor, Commands, PublicSpace, **Subscriber**, Help, and Exit. The main area has tabs: Billing, **Messages**, and Authorized. Under the Messages tab are sub-tabs: **Login Msgs**, Sub Msgs 1, Sub Msgs 2, Sub Msgs 3, Error Msgs 1, and Error Msgs 2. The Login Msgs tab contains the following text: "This tab is used to customize presentation and content of subscriber's login User Interface (UI)" and "Note: Reboot is required for image file name change to take effect." Below this is the "Subscriber Login Messages" section with a list of parameters and their values:

Service Selection Message	Please select the amount of high-speed access you wish t
Existing User Name Message	Please enter your user ID and password:
New User Name Message	Please enter a new user ID and password:
Contact Message	Please contact your Network Administrator in case of prob
Enable JavaScript	<input checked="" type="checkbox"/>
Enable "Remember Me" option	<input checked="" type="checkbox"/>
"Remember Me" Message	Remember my username and password.
Remember for how many days	7
Currency	\$
Number of decimals for amount	2
Image File Name	hotspot.gif
Enable Partner Image	<input type="checkbox"/>
Partner Image File Name	

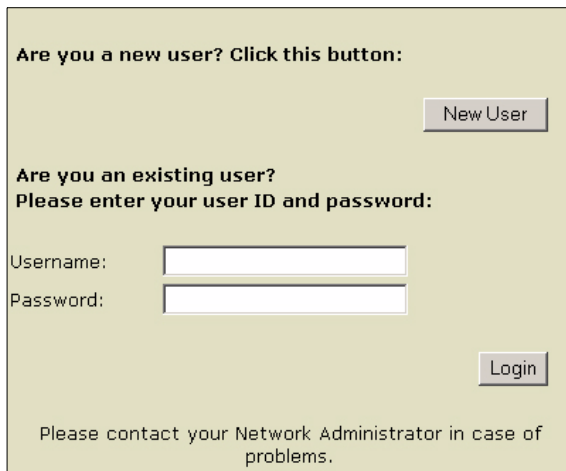
At the bottom of the form are "OK" and "Cancel" buttons.

Figure 5-31 Subscriber Login Messages

3. Edit the login messages as necessary.

- **Service Selection Message**
- **Existing User Name Message**
 - Appears on the main login screen when the **User Name** option is enabled in **PublicSpace > AAA > Internal**.
 - Default is "Please enter your user ID and password".
- **New User Name Message**
 - Appears on the **New User** screen when the **User Name** and **New Subscribers** options are enabled in **PublicSpace > AAA > Internal**.
 - Default is "Please enter a new user ID and password".
- **Contact Message**
 - Appears on all internal Web pages.
 - Default is "Please contact your Network Administrator in case of problems."
- A sample login screen (without the logo) is shown below.

Public Space Parameters



The image shows a login screen with a light beige background. At the top, it asks 'Are you a new user? Click this button:' with a 'New User' button. Below that, it asks 'Are you an existing user? Please enter your user ID and password:'. There are two input fields: 'Username:' and 'Password:'. A 'Login' button is at the bottom right. At the bottom, it says 'Please contact your Network Administrator in case of problems.'

Figure 5-32 Sample Login Screen Presented to Subscribers

4. JavaScript support on the AP's internal Web pages are enabled by default. Remove the check mark from the **Enable JavaScript** to disable this feature.
5. Configure the "Remember Me" cookie options. See [Enabling Cookie Support](#) for details.
6. Define the currency label for the billing plans (for example, \$) in the **Currency** field.
7. Enter a numeric value for the **Number of decimals for amount**. This field defines the number of decimal places that are shown for the displayed amounts.
8. Configure the images that appear on the login screens and on the connection screen. See [Changing the Login Screen Logos](#).
9. Click the **Sub Msgs 1** tab.
10. Edit the subscriber messages as necessary.
 - **Please select the Billing Mode**
 - **Bill by Credit Card**
 - **Choose a User ID (optional)**
 - This text appears on the **New User** screen if the **User Name** and **New Subscribers** options are enabled in **PublicSpace > AAA > Internal**.
 - **Choose a Password ID (optional)**
 - This text appears on the **New User** screen if the **User Name** and **New Subscribers** options are enabled in **PublicSpace > AAA > Internal**.
 - **Retype the Password (if entered above)**
 - This text appears on the **New User** screen if the **User Name** and **New Subscribers** options are enabled in **PublicSpace > AAA > Internal**.
 - **Free access to the Internet**
 - **Are you a new user? Click this button**
 - This text appears on the main login screen if the **New Subscribers** option is enabled in **PublicSpace > AAA > Internal**.
 - **Are you an existing user?**
 - This text appears on the main login screen if the **User Name** option is enabled in **PublicSpace > AAA > Internal**.



NOTE

Some messages only appear when certain features are enabled.

11. Click **OK**.

Public Space Parameters

The screenshot shows a web-based configuration interface for a Proxim Wireless Network. On the left is a vertical sidebar with buttons: Status, Configure, Monitor, Commands, PublicSpace, **Subscriber** (highlighted in orange), Help, and Exit. The main area has a top navigation bar with tabs: Billing, **Messages** (highlighted in orange), and Authorized. Under the Messages tab, there are sub-tabs: Login Msgs, **Sub Msgs 1** (highlighted in orange), Sub Msgs 2, Sub Msgs 3, Error Msgs 1, and Error Msgs 2. The content area for Sub Msgs 1 contains the following text and form fields:

This tab is used to define various subscriber messages to be displayed to subscriber

Subscriber Messages

Please select the Billing Mode

Please select the Billing Mode:

Bill by Credit Card

Bill by Credit Card:

Choose a User ID (optional)

Choose a User ID (optional)

Choose a Password (optional)

Choose a Password (optional)

Retype the Password (if entered above)

Retype the Password (if entered above)

Free access to the Internet

Free access to the Internet:

Are you a new user? Click this button

Are you a new user? Click this button:

Are you an existing user?

Are you an existing user?

At the bottom right of the form are two buttons: OK and Cancel.

Figure 5-33 Subscriber Messages Screen

12. Click the **Sub Msgs 2** tab.
13. Edit the subscriber messages as necessary.
 - **If this is not correct, please go back to the previous page**
 - **and make the necessary changes**
 - **Please select purchase time**
 - **Purchase one-time access using your credit card**
 - **If you want to create a new account**
 - **If you have an existing account**
 - **Your request was declined**
 - **Your request was successful**



NOTE

Some messages only appear when certain features are enabled.

14. Click **OK**.
15. Click the **Sub Msg 3** tab.

Public Space Parameters

16. Edit the subscriber messages as necessary.
 - **Thank you for your business**
 - **We are verifying your account. Please wait**
 - This message appears if RADIUS is enabled. The AP displays this page while it wait for an authentication response from the RADIUS server.
 - **You will be purchasing Internet access with these options**
 - This message appears on the final credit card purchase screen before the customer is directed to the credit card service provider.



NOTE

Some messages only appear when certain features are enabled.

17. Click **OK**.
18. Click the **Error Msgs 1** tab.
19. Edit the error messages as necessary. The AP will display one of these error messages to the subscriber if a problem occurs during the login process.
 - **Access point blocked subscriber access**
 - **Access to this document requires a password**
 - **An error has occurred**
 - **You received a challenge from your Internet Service Provider**
 - **This field must contain a number between these two values**
 - **No Billing options are available**
 - **Internet Service is not available right now. Try again later**
 - **The password fields you have entered do not match. Please try again**
 - **The password field you have entered is not correct. Please try again**
20. Click **OK**.
21. Click the **Error Msgs 2** tab.
22. Edit the error messages as necessary. The AP will display one of these error messages to the subscriber if a problem occurs during the login process.
 - **Too many subscribers are already logged in. Please try again later**
 - **Try again**
 - **The User ID you have entered cannot be found. Please try another**
 - **The User ID you have entered is already taken. Please try another**
 - **We are sorry**
 - **This field must contain a whole number value, with no decimals**
 - **Your account was not found. Please check your User name and Password**
23. Click **OK**.
24. Reboot the AP.

Enabling Cookie Support

The AP can store an encrypted login cookie in the subscriber's browser to facilitate future logins.

When enabled, the AP stores a cookie in the subscriber's browser when the customer selects the **Remember my username and password** option during login. The next time the customer connects to the network, the cookie contains all of the necessary login information so the customer is automatically logged in without having to re-enter his user name and password.

Follow these steps if you want to provide cookie support to your subscribers:

1. Login to the AP's Web browser interface.
2. Click **Subscriber > Messages > Login Msgs**.
3. Place a check mark in the **Enable "Remember Me"** option.

Public Space Parameters

4. Edit the **Remember Me Message**.
 - This message appears on the login screen to let the user know that his/her user name and password can be stored for future login attempts.
 - The default message is “Remember my username and password.”
5. Enter the number of days for which the cookie will be valid in the **Remember for how many days** field.
6. Click **OK**.

Changing the Login Screen Logos

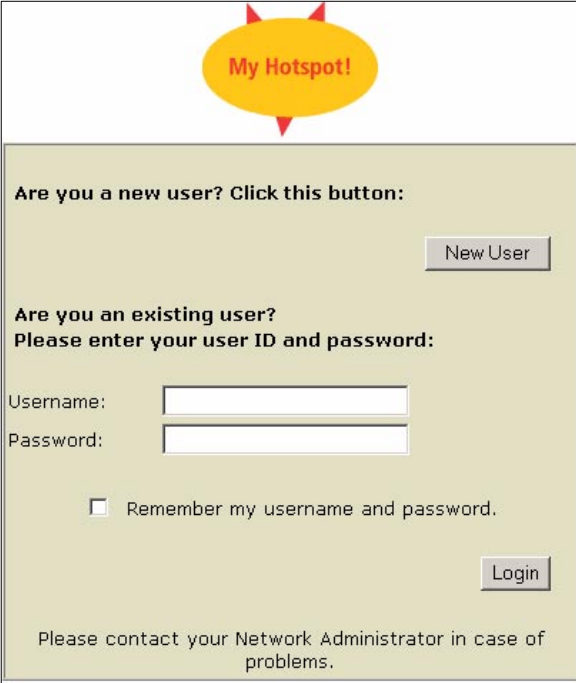
By default, two images appear on the AP's internal login screen. One is the connecting image that appears when a subscriber first opens the browser. It is a green swirl that reads: “You are being connected.” You cannot change this image but you can add your own image to this screen (this is known as a “partner image”). The following sample page includes a partner image (the “myhotspot” logo):



Figure 5-34 Connecting Screen with Partner Image

The second image that appears on the AP's internal web pages is the default logo. This logo appears at the top of each login page. The following sample page includes the custom “myhotspot” logo.

Public Space Parameters



The image shows a login screen for a Proxim wireless network. At the top, there is a yellow speech bubble with the text "My Hotspot!". Below this, the screen is divided into two sections. The first section asks "Are you a new user? Click this button:" and features a "New User" button. The second section asks "Are you an existing user? Please enter your user ID and password:". It contains two input fields, one for "Username:" and one for "Password:". Below these fields is a checkbox labeled "Remember my username and password." and a "Login" button. At the bottom of the screen, there is a note: "Please contact your Network Administrator in case of problems."

Figure 5-35 Login Screen with Custom Logo

Follow these steps to add your own partner image and logo to the AP:

1. Create the image files that you want to add to the login pages. Keep in mind the following:
 - The file should be in JPG or a GIF format.
 - The file name cannot exceed 8 characters (DOS 8+3 format).
 - The logo image (that is, the logo that appears on each login screen) should not be too large. The recommended size is approximately 125 pixels wide by 40 pixels high.
 - The partner image for the connecting screen can be larger than the logo image.
 - For each file, you may want to try out multiple image sizes before you settle on one particular size.
2. Copy the image files to your TFTP server's root directory.
3. Login to the AP's Web browser interface.
4. Click **Commands > Download**.
5. Use the [Download](#) command to download the image files to the AP.
 - Enter the file name in the **File Name** field. Remember that the name cannot exceed 8 characters (not including the extension).
 - The File Type is **Generic**.
6. Click **Subscriber > Messages > Login Msgs**.
7. Enter the name of logo image you downloaded to the AP in the **Image File Name** field.
8. Place a check mark in the **Enable Partner Image** box.
9. Enter the file name of the partner image you downloaded to the AP in the **Partner Image File Name** field.
10. Click **OK**.
11. Reboot the AP.

Authorized Subscribers

The AP-2500 stores information about subscribers in the Authorized Subscribers Table. You can view the table by clicking **Subscriber > Authorized** within the Web browser interface.



Name	Mac	IP	BwUp	BwDown	AmtPaid	AmtLeft	Status
dfgdfgdfgdfg	01:01:11:11:11:11	2.2.2.2	123	1231	1231.00	0.00	Active
sdfsd	11:11:11:11:11:11	22.11.22.11	1111	1111	123.00	0.00	Active
releaseimage	12:12:12:12:12:12	1.2.1.2	123	123	123.00	0.00	Active
test2	22:22:22:22:22:22	5.6.7.8	1001	1001	100.00	0.00	Active
release_1	22:33:33:33:33:33	3.3.3.3	123	213	123.00	0.00	Active
test3	33:33:33:33:33:33	11.11.11.11	1001	1001	100.00	0.00	Active
test4	44:44:44:44:44:44	1.2.3.4	1001	1001	100.00	0.00	Active
test5	55:55:55:55:55:55	55.55.55.55	1001	1001	100.00	0.00	Active
raman	66:66:66:66:66:66	1.2.3.4	1001	1001	100.00	0.00	Active
jen	77:77:77:77:77:77	1.2.3.4	1001	1001	100.00	0.00	Active
super	88:88:88:88:88:88	5.6.7.8	1001	1001	100.00	0.00	Active
testanilnaik	99:99:99:99:99:99	11.22.33.44	1001	1001	100.00	0.00	Active

Figure 5-36 Authorized Subscribers Table

The table is the AP's internal database of authorized users; it can hold up to 50 entries. The list is populated by one of three methods:

1. Automatically following a successful credit card transaction.
2. Manually by a network administrator.
3. Using XML commands (see [XML Interface Specification](#) for details).

From the main table screen you can view the following information about each subscriber:

- User Name (if applicable)
- MAC address of user's wireless card
- User's IP address
- User's Upstream and Downstream bandwidth settings
- The monetary amount paid by the customer
- The monetary amount remaining in the user's account (if applicable)
- The user's status (should be **Active** at all times when in the Authorized Subscribers Table)

Click **Edit** to view additional information about the subscriber. You can also edit certain parameters from this screen. The following information is available about each subscriber in the **Modify Authorized Subscriber Details** screen:

- DHCP Address Type (Public or Private)
- MAC address of user's wireless card (for viewing only)
- User's IP address
- User Name
- Password
- Amount of time remaining in the account (**Expiration Time** fields)
- Amount Paid by user

Public Space Parameters

- Custom fields for internal use (User Alias 1 or User Alias 2)
- Upstream and Downstream bandwidth settings
- Status
 - Should be **Active** at all times.
 - Change to **Destroy** to delete an entry.
 - The other options are not applicable when using the Web browser interface.

Authorized Subscribers Table and the Current Subscribers Table

The Authorized Subscribers Table differs from the [Current Subscribers Table](#), found in the **Monitor > Subscribers** screen. The Current Subscribers Table only lists those users who are currently connected to the AP.

Therefore, an active user who purchased access time with a credit card will appear in both the Authorized Subscribers Table and the Current Subscribers Table. When using internal authentication with RADIUS, an active user authenticated by a RADIUS server appears only in the Current Subscribers Table (RADIUS-authenticated users never appear in the Authorized Subscribers Table). When using external authentication with XML, an active user will appear in both the tables (the USER_ADD command adds the user to the Authorized Subscribers Table and the UPDATE_CACHE command changes the user's Current Subscribers State from "Pending" to "Valid"; see [XML Interface Specification](#) for details).

If a user appears in both tables, deleting the user from one table will automatically remove the user from the second table.

Also, rebooting the AP will clear the Current Subscribers Table but not the Authorized Subscribers Table. (The Authorized Subscribers information is retained in non-volatile memory.)

Manually Adding a Subscriber

Follow these steps to manually add a subscriber to the Authorized Subscribers Table:

1. Login to the AP's Web browser interface.
2. Click **Subscriber > Authorized**.
3. Click **Add**.

Figure 5-37 Add a Subscriber Screen

4. Select the **DHCP Address Type** for the subscriber (public or private). This setting depends upon the [DHCP Server](#) settings you configured for the AP.

Public Space Parameters

5. If authorizing a user based on MAC address (in other words, the **PublicSpace > AAA > Internal > Enable User Name** option is disabled), enter the MAC address of the subscriber's wireless card in the field provided.
 - If you have chosen to manage this subscriber by user name only, you do not need to enter a MAC address (however, you will need to enter a user name).
6. Enter an **IP Address** for the subscriber or leave the field blank.
 - If left blank, the AP fills in this field automatically after a subscriber logs in.
7. If authorizing a subscriber based on user name and password, enter a **User Name** and **Password** for the subscriber in the fields provided.



NOTE

User Name and Passwords are case-sensitive.

8. Enter the subscriber's allowed access time in the **Expiration Time** fields (in hours and/or minutes).
 - If you leave these fields blank or set them to 0, the subscriber will never time out.
 - If you enter hours and/or minutes, the timeout counter will begin as soon as you click **OK**.
 - After the subscriber has timed out, he/she must re-subscribe to the service.
9. Configure the **Amount Paid** field, if desired. The AP automatically fills in this fields after a successful credit card purchase.
10. Configure the optional **User Alias** fields, if desired. These are for notes only and do not have an impact on the authentication process.
11. Define the **Upstream** and **Downstream Bandwidth** limits for the user in Kbps. The user's bandwidth is not limited if you leave this blank or set it to 0.
12. Click **OK** to add the subscriber.
13. Add additional subscribers, if desired.
14. When finished, click the back arrow button to return to the previous screen.

Removing a Subscriber

Follow these steps to remove a subscriber from the Authorized Subscribers Table:

1. Login to the AP's Web browser interface.
2. Click **Subscriber > Authorized**.
3. Click **Edit**.
4. Locate the entry for subscriber you want to delete and set **Status** to **Destroy**.
5. Click **OK** to remove the entry.
6. Click the back arrow button to return to the previous screen.



NOTE

An active subscriber will immediately lose his/her access to the Internet if the subscriber's entry is deleted. You can also delete active subscribers from **Monitor > Subscribers**. See [Current Subscribers Table](#).

6

Monitor Information

In This Chapter

This chapter describes the statistics that can be viewed using the Access Point's Web browser interface (that is, the options accessible after clicking the **Status** or **Monitor** button).

- [System Status](#): Displays basic information about the Access Point's operating status.
- [Version](#): Provides version information for the Access Point's system components.
- [ICMP](#): Displays statistics for Internet Control Message Protocol packets sent and received by the Access Point.
- [IP/ARP Table](#): Displays the Access Point's IP Address Resolution table.
- [Learn Table](#): Displays the list of nodes that the Access Point has learned are on the network.
- [Current Subscribers Table](#): Displays the list of current subscribers
- [DAT Sessions](#): Displays the list of current Dynamic Address Translation (DAT) sessions
- [Interfaces](#): Displays the Access Point's interface statistics (Wireless and Ethernet).
- [Link Test \(802.11b Only\)](#): Evaluates the link with a wireless client.



NOTE

See [Logging into the Web Interface](#) for instructions on how to access the AP's Web browser interface.

Monitor Information

System Status

System Status is the first screen to appear each time you connect to the Web browser interface. You can also return to this screen by clicking the **Status** button.

Status

System Status APv1.0.0 SN-03UT11570395 v2.0.10

IP Address	192.168.0.3	Contact Name	Contact Name
System Name	Wireless LAN AP	Contact Phone	Contact Phone Number
System Location	Contact Location	Contact Email	name@Organization.com
Up Time (DD:HH:MM:SS)	00:01:05:05	Object ID	1.3.6.1.4.1.11898.2.4.11

System Alarms

This table displays information on the alarms (SNMP Traps) generated by the access point. They should be deleted once they are reviewed and resolved. The alarm severity levels are: Critical, Major, Minor, and Informational.

	Description	Severity	Time Stamp
<input type="checkbox"/>	AP Cold Started.	Informational	0 days 0 hrs 0 m 21 s
<input type="checkbox"/>	Link Up.	Informational	0 days 0 hrs 0 m 21 s
<input type="checkbox"/>	Link Up.	Informational	0 days 0 hrs 0 m 21 s
<input type="checkbox"/>	Link Up.	Informational	0 days 0 hrs 0 m 21 s
<input type="checkbox"/>	Link Up.	Informational	0 days 0 hrs 0 m 21 s

Figure 6-1 System Status Screen

Each section of the **System Status** screen provides the following information:

- **System Status:** This area provides system level information, including the unit's IP address and contact information. See [System](#) for information on these settings.
- **System Alarms:** System traps (if any) appear in this area. Each trap identifies a specific severity level: Critical, Major, Minor, and Informational. See [System Alarms \(Traps\)](#) for a list of possible alarms.
 - To delete an alarm, place a check mark in the box to the left of its entry and click **Delete**.
 - To delete all alarms reported on screen, click **Select All** and click **Delete**.

Monitor Information

Version

From the Web browser interface, click the **Monitor** button and select the **Version** tab. The list displayed provides you with information that may be pertinent when calling Technical Support. With this information, your Technical Support representative can verify compatibility issues and make sure the latest software are loaded. This screen displays the following information for each Access Point component:

- **Serial Number:** The component's serial number, if applicable.
- **Component Name**
- **ID:** The AP identifies a system component based on its ID. Each component has a unique identifier.
- **Variant:** Several variants may exist of the same component (for example, a hardware component may have two variants, one with more memory than the other).
- **Version:** Specifies the component's version or build number. The Software Image version is the most useful information on this screen for the typical end user.

Serial Number	Name	ID	Variant	Version
Not Applicable	Software Image	89	1	1.0.0
03UT11570395	Hardware Inventory	97	1	1.0
Not Applicable	AP- Firmware	842	1	8.42
Not Applicable	BSP-BL Original	111	1	2.0.10
Not Applicable	ORINOCO MIB	122	1	3.22
Not Applicable	Config File	121	1	3.1
Not Applicable	Wireless Card A-PRI Firmware	0	0	0.0
Not Applicable	Wireless Card A-NIC	0	0	0.0
Not Applicable	Wireless Card B-PRI Firmware	21	1	4.4
03UT11417696	Wireless Card B-NIC	1	1	4.2

Figure 6-2 Version Information Screen

ICMP

This tab provides statistical information for both received and transmitted messages directed to the Access Point. For example, if you ping the AP from another computer, the AP reports the ping requests (Echos) and replies (Echo Reply) on this screen (as shown in the example below). Not all ICMP traffic on the network is counted in the ICMP (Internet Control Message Protocol) statistics.



NOTE

To update the statistics, click the **Refresh**  button.



Messages Received		Messages Transmitted	
Total ICMP Packets	4	Total ICMP Packets	4
Errors	0	Errors	0
Destination Unreachable	0	Destination Unreachable	0
Time Exceeded	0	Time Exceeded	0
Parameter Problems	0	Parameter Problems	0
Source Quench	0	Source Quench	0
Redirects	0	Redirects	0
Echos	4	Echos	0
Echo Reply	0	Echo Reply	4
Time Stamps	0	Time Stamps	0
Time Stamp Reply	0	Time Stamp Reply	0
Address Mask	0	Address Mask	0
Address Mask Reply	0	Address Mask Reply	0

Figure 6-3 ICMP Monitoring Screen

Monitor Information

IP/ARP Table

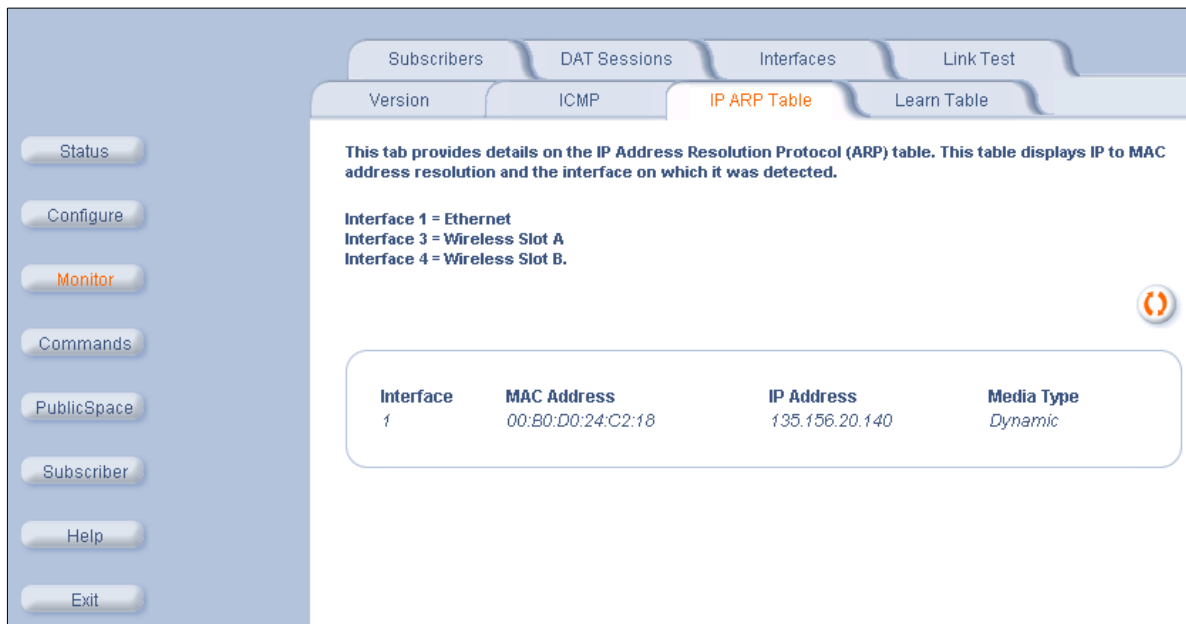
This tab provides information based on the Address Resolution Protocol (ARP), which maps IP Addresses to MAC Addresses. The AP adds an entry to this list for each station with which the AP directly communicates. This includes devices that manage the AP, ping the AP, and/or receive traps from the AP. The AP does not create an entry for every station it detects on the network.

An entry times out after five minutes of inactivity (that is, after five minutes of no communication between the device and the AP).



NOTE

To update the table, click the **Refresh**  button.



The screenshot shows the Proxim Wireless Networks web interface. On the left is a sidebar with buttons: Status, Configure, Monitor (highlighted in orange), Commands, PublicSpace, Subscriber, Help, and Exit. The main content area has tabs: Subscribers, DAT Sessions, Interfaces, Link Test, Version, ICMP, IP ARP Table (highlighted in orange), and Learn Table. Below the tabs, a text box explains the ARP table. Below that, a table displays the current ARP entry. A Refresh button (circular arrow icon) is located to the right of the table.


This tab provides details on the IP Address Resolution Protocol (ARP) table. This table displays IP to MAC address resolution and the interface on which it was detected.

Interface 1 = Ethernet
Interface 3 = Wireless Slot A
Interface 4 = Wireless Slot B.

Interface	MAC Address	IP Address	Media Type
1	00:B0:D0:24:C2:18	135.156.20.140	Dynamic


Figure 6-4 IP/ARP Table

Learn Table

This tab displays information relating to network bridging. It reports the MAC address for each node that the AP has learned is on the network and the interface on which the node was detected. There can be up to 2,000 entries in the Learn Table. Click the **Refresh**  button if you want to update the table.

For this screen, Port 1 is Ethernet interface. Port 2 is the Slot A interface. Ports 3 through 8 are WDS ports for Slot A (if applicable). Port 9 is the Slot B interface. Ports 10 through 15 are WDS ports for Slot B (if applicable).

In the example below, the AP has two wireless clients in its Learn Table; both clients are associated with the radio in Slot B.



MAC Address	Port
00:B0:D0:24:C2:18	1
00:02:2D:57:9C:5F	9
00:02:2D:2F:6B:D3	9

Figure 6-5 Learn Table

Monitor Information

Current Subscribers Table

This table lists all of the active subscribers that are communicating with the AP. (See [Authorized Subscribers Table](#) and [the Current Subscribers Table](#) for an explanation of how this table differs from the Authorized Subscribers Table.) This table can hold up to 50 entries.

Users who are associated with the AP wirelessly but are unauthenticated appear in the table with **State** set to **Pending**. Once a user has been authenticated (by the AP, a RADIUS server, or an External Web Server), the AP updates the user's entry and changes the **State** to **Valid**.

The AP reports the following information for each subscriber:

- **User Name** (if applicable)
- **IP address** of user's wireless card
 - In the example below, *dcrispin* received an IP address from the AP via DHCP and *Edgar* is using a static IP address (but the AP's DAT functionality accounts for this and the user is unaware that his IP address is misconfigured for the hotspot's network).
- **MAC address** of user's wireless card
- **State**
 - Set to **Pending** for devices that have associated to the AP wirelessly but are not yet authenticated.
 - Set to **Valid** after a device or user has been authenticated.
- **Proxy**
 - Reports if the AP detected proxy server settings on the subscriber's Web browser and is redirecting the traffic as necessary
- **BwUp**: Subscriber's upstream bandwidth limit
- **BwDown**: Subscriber's downstream bandwidth limit
- **BytesSent**: Number of bytes sent by the subscriber (upstream)
- **Bytes Received**: Number of bytes received by the subscriber (downstream)
- **BytesTotal**: Sum of BytesSent and BytesReceived
- **Status**
 - Should be **Active** at all times.
 - Change to **Destroy** to delete an entry.



Figure 6-6 Current Subscribers Screen

Monitor Information

A subscriber is removed from the Current Subscribers Table under the following circumstances:

- The network administrator changes the subscriber's **Status** from **Active** to **Destroy**.
- The subscriber has logged out (applicable to RADIUS-authenticated users and **RADIUS Profile Caching** is disabled).
- The amount of access time purchased by the subscriber has expired.
 - Users authenticated by the Authorized Subscribers Table whose expiration time expires are reset to **State: Pending**.
- The subscriber's entry times out after a period of inactivity.
 - RADIUS-authenticated users time out based on the Default Idle Timeout setting, the Idle-Timeout attribute, or the Session-Timeout attribute.
 - Pending users and users authenticated by the Authorized Subscribers Table whose time has not expired are removed from the table approximately 10 minutes after the subscriber's wireless card disconnects from the AP (for example, when the user leaves the hotspot).

DAT Sessions

The AP performs Dynamic Address Translation (DAT) to provide subscribers with access to the Internet. See [Dynamic Address Translation \(DAT\)](#) for details.

The **Current Subscriber DAT Sessions** screen displays the active DAT sessions for each subscriber. The subscriber is identified by the IP address and MAC address of his/her wireless card.

The **SubPort** identifies the source port that the subscriber is using; the **NetPort** identifies the port that the AP maps with its IP address to send out the subscriber's packet.

For UDP sessions, the **SessState** is MAPPED (meaning the subscriber's port has been mapped to a port on the AP for address translation purposes).

For TCP sessions, the **SessState** is ESTABLISHED (for open connections), TIME WAIT (for pending connections), or CLOSED (for closed connections).

Version ICMP IP ARP Table Learn Table							
Subscribers DAT Sessions Interfaces Link Test							
Status Configure Monitor Commands PublicSpace Subscriber Help Exit							
Current Subscriber DAT Sessions The access point DAT (Dynamic Address Translation) feature allows all users to obtain network access regardless of their computer's network settings. The table below displays currently active DAT sessions.							
SubIP	SubPort	SubMac	NetPort	NetProtocol	SessState	Timeout	
10.0.0.15	137	00-20-A6-4B-FF-1E	5001	UDP	MAPPED	471	
10.0.0.15	138	00-20-A6-4B-FF-1E	5002	UDP	MAPPED	366	
10.0.0.15	1280	00-20-A6-4B-FF-1E	5003	TCP	TIME WAIT	3978	
10.0.0.15	1291	00-20-A6-4B-FF-1E	5004	TCP	CLOSED	3860	
172.45.23.12	1401	00-02-2D-51-94-E4	5027	TCP	TIME WAIT	184	
172.45.23.12	1410	00-02-2D-51-94-E4	5028	TCP	CLOSED	164	
172.45.23.12	138	00-02-2D-51-94-E4	5029	UDP	MAPPED	76	
172.45.23.12	1419	00-02-2D-51-94-E4	5030	TCP	CLOSED	134	
172.45.23.12	1421	00-02-2D-51-94-E4	5031	TCP	CLOSED	132	
172.45.23.12	1422	00-02-2D-51-94-E4	5032	TCP	CLOSED	132	
172.45.23.12	1424	00-02-2D-51-94-E4	5033	TCP	CLOSED	121	
172.45.23.12	1425	00-02-2D-51-94-E4	5034	TCP	CLOSED	121	

Figure 6-7 Current Subscriber DAT Sessions Screen

Monitor Information

Interfaces

This tab displays statistics for the Ethernet and wireless interfaces. The Operational Status can be up, down, or testing.

Version **ICMP** **IP ARP Table** **Learn Table**

Subscribers **DAT Sessions** **Interfaces** **Link Test**

Status **Configure** **Monitor** **Commands** **PublicSpace** **Subscriber** **Help** **Exit**

This tab provides information and statistics on the access point's Ethernet interface.

Ethernet

Type: ethernet-csmacd
Description: 0.0

Version **ICMP** **IP ARP Table**

Subscribers **DAT Sessions** **Interfaces**

This tab displays information and statistics on the access point's Wireless interface.

Wireless - Slot B

Type: ethernet-csmacd
Description: 0.0
MIB Specific Definition: wlc1
MAC Address: 00:02:2D:29:D7:98
Last Change: 9302300
Operational Status: Up
Admin Status: Up
Speed: 11000000
Maximum Packet Size: 1500
In Octets (bytes): 92311
In Unicast Packets: 76
In Non-unicast Packets: 739
In Discards: 0
In Errors: 0
Unknown Protocols: 0
Out Octets (bytes): 1021435
Out Unicast Packets: 12
Out Non-unicast Packets: 19960
Out Discards: 0
Out Errors: 0
Output Queue Length: 10
Transmitted Fragment Count: 911233
Multicast Transmitted Frame Count: 236
Failed Count: 547
Retry Count: 0
Multiple Retry Count: 547
Duplicate Frame Count: 0
Successful RTS Count: 0
Failed RTS Count: 0
Failed ACK Count: 0
Received Fragment Count: 90539
Multicast Received Frame Count: 560
FCS Error: 187991
Transmitted Frame Count: 265
WEP Undecryptable Count: 0

Figure 6-8 Interface Monitoring

Monitor Information


Link Test (802.11b Only)

This tab displays information on the quality of the wireless link to clients and other 802.11b APs in the Wireless Distribution System. During a Link Test, the Access Point and the selected device exchange a series of packets to test the strength of the connection. The devices start by exchanging packets at the 11 Mbits/sec rate but fall back to the slower rates if necessary.

NOTE

The Remote Link Test feature is only available for 2.4 GHz (802.11b) clients. Also, this feature is not available if you are using an ORINOCO 802.11a/b ComboCard or a non-ORINOCO client.

Follow these steps to perform a Link Test:

1. Login to the AP's Web browser interface.
2. Click **Monitor > Link Test**.
3. Click **Explore**.
 - Result: A list of detected stations will appear. If the list does not appear automatically, click **Refresh** .

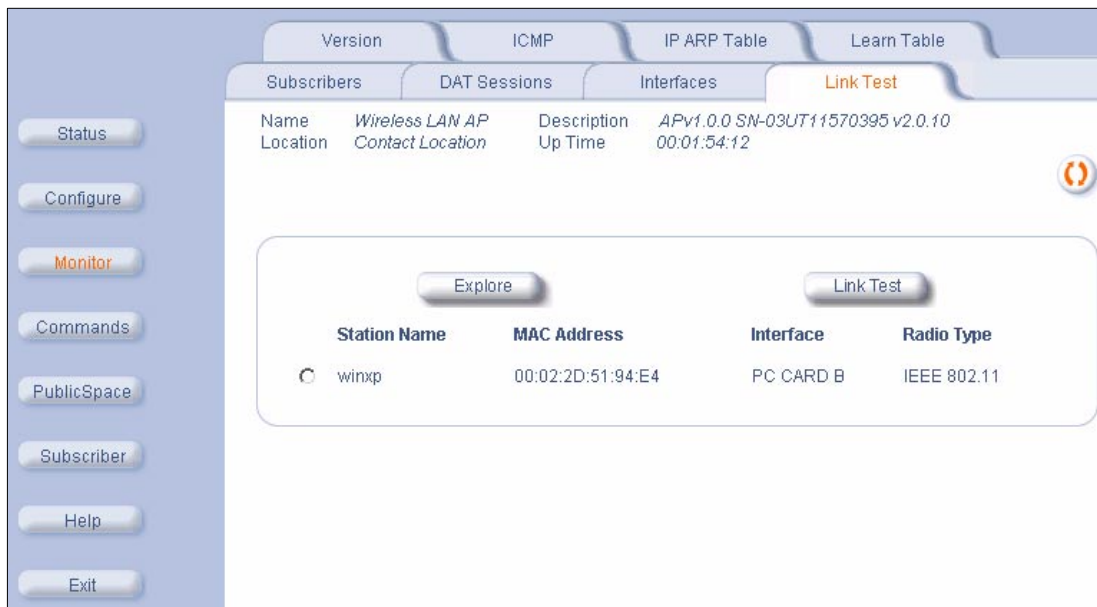


Figure 6-9 Remote Link Test Screen

4. Select a Station from the list by clicking the circle to the left of the Station's entry.
5. Click **Link Test** to start the test.
 - Result: A new Link Test window opens and displays the following information for the Access Point (referred to as the **Initiator Station**) and the wireless client (referred to as the **Remote Station**):
 - **Station Name:** The Access Point's System Name or the client's Windows Networking name.
 - **MAC Address**
 - **SNR (dB):** The Signal to Noise ratio for the received signal. The displayed value is the running average since the start of the test and is reported in decibels (dB). Higher numbers correspond to a stronger link. The bar graph also displays the relative strength of the link (a green bar indicates a strong link, a yellow bar indicates a fair link, and a red bar indicates a weak link).
 - **Signal (dBm):** The strength of the received signal in dBm (decibels referenced to 1 milliwatt). The displayed value is the running average since the start of the test and is reported as a negative number. Higher numbers correspond to a stronger link. For example, -40 dBm corresponds to a stronger signal than -50 dBm. The bar graph also displays the relative strength of the signal (a longer bar represents a stronger signal).

Monitor Information

- **Noise (dBm):** The strength of the noise detected at the receiver reported in dBm (decibels referenced to 1 milliwatt). The displayed value is the running average since the start of the test and is reported as a negative number. Noise can interfere with the received signal so a smaller noise value corresponds to a stronger link. For example, a noise level of -95 dBm is more desirable than a noise level of -89 dBm. The bar graph displays the relative strength of the noise level (a shorter bar represents a weaker noise level and is more desirable than a longer bar).
- **11 Mbps (pkts):** The number of packets received at the 11 Mbps/sec transmit rate since the start of the Link Test. In general, most packets will be received at the 11 Mbps/sec rate if the devices have a strong link.
- **5.5 Mbps (pkts):** The number of packets received at the 5.5 Mbps/sec transmit rate since the start of the Link Test.
- **2 Mbps (pkts):** The number of packets received at the 2 Mbps/sec transmit rate since the start of the Link Test.
- **1 Mbps (pkts):** The number of packets received at the 1 Mbps/sec transmit rate since the start of the Link Test.



NOTE

Click the **Refresh**  button periodically to update the test results. The test screen does not refresh automatically.

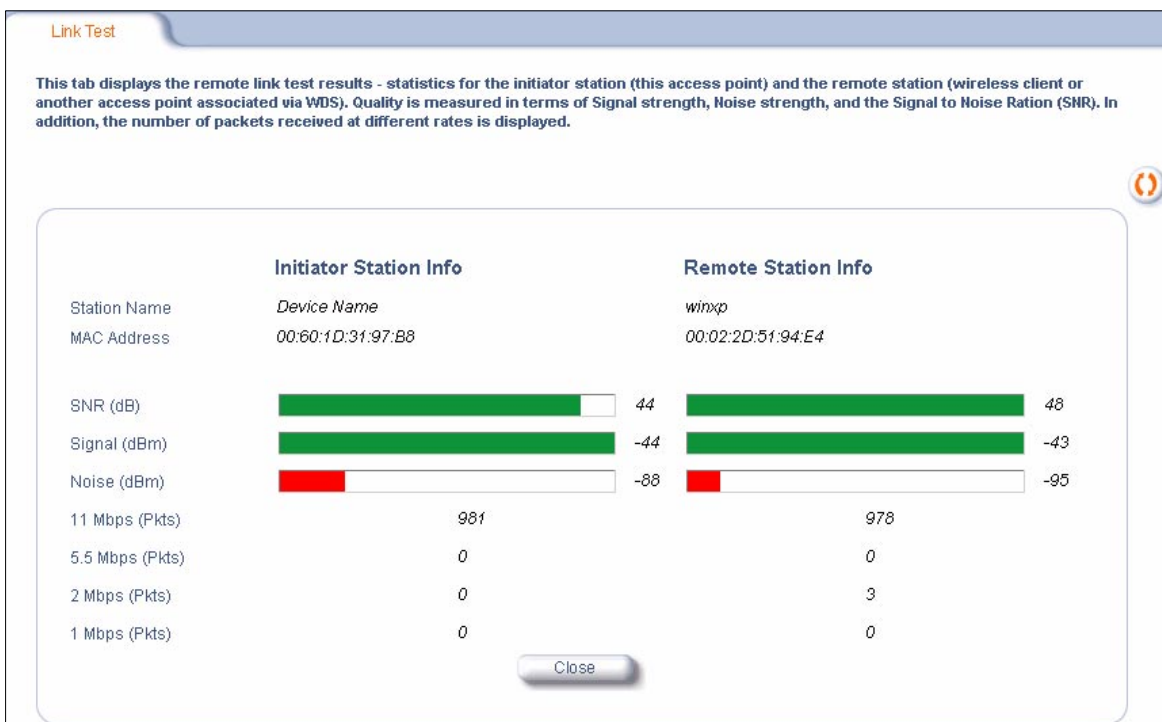


Figure 6-10 SNR Report Screen

6. Click **Close** to end the Link Test.

Commands

In This Chapter

This chapter describes the commands that can be issued using the Access Point's Web browser interface (that is, the options accessible after clicking the **Commands** button).

- **Download:** Download files from a TFTP server to the Access Point.
- **Upload:** Upload files from the Access Point to a TFTP server.
- **Reboot:** Reboot the Access Point in the specified number of seconds.
- **Reset:** Reset all of the Access Point's configuration settings to factory defaults.
- **Help Link:** Configure the location where the Access Point's Help files can be found.

⇒ NOTE

See [Logging into the Web Interface](#) for instructions on how to access the AP's Web browser interface.

Download

Use the **Download** tab to download AP Image, Bootloader, Configuration, and Generic files from a TFTP server to the Access Point.

⇒ NOTE

The **Download** and **Upload** commands are from the AP's perspective. In other words, to send files to the AP, use the Download command; to obtain files from the AP, use the Upload command.

A TFTP server must be running and configured to point to the directory containing the file. If you don't have a TFTP server installed on your system, install the TFTP server from the ORiNOCO CD. You can either install the TFTP server from the CD Wizard or run **OEM-TFTP-Server.exe** found in the CD's *Xtras/SolarWinds/* sub-directory.

The screenshot shows the 'Download' tab selected in the 'Commands' section of the web interface. The interface has a sidebar on the left with buttons for Status, Configure, Monitor, Commands (highlighted), PublicSpace, Subscriber, Help, and Exit. The main content area has tabs for Download, Upload, Reboot, Reset, and Help Link. Below the tabs, a message states: 'This tab is used to download software and configuration files from a TFTP server to the access point. This can be used for software upgrades.' The 'System Information' section shows 'Software Version: 1.0.0' and 'Boot Loader Version: 2.0.10'. The 'TFTP Information' section contains four fields: 'Server IP Address' (192.168.0.101), 'File Name' (current.bt), 'File Type' (Generic), and 'File Operation' (Download). At the bottom right are 'OK' and 'Cancel' buttons.

Figure 7-1 Download Command Screen

File Type Overview

For Downloads, the **File Type** parameter supports four options: Config, Img, BspBI, and Generic. For Uploads, **File Type** supports two options: Config and Generic.

- **Config:** This refers to a file that contains the AP's network configuration settings (that is the parameters that correspond to the ORiNOCO MIB; see [SNMP Management](#) for details).
 - You can download the current configuration settings from the AP for back-up purposes or upload a configuration file to the AP so it adopts the settings contained in the file. See [Back-up the AP's Configuration Files](#) for details.
 - You can use any name for the config file. Proxim recommends using **config.sys**.
- **Img:** This refers to the AP's firmware image.
 - This File Type only supports the Download command. You cannot upload the AP's firmware image file to a TFTP server.
 - Proxim periodically makes new firmware available on its Web site that you can download to the AP using a TFTP server; see [Download the Latest Software](#) for instructions.
- **BspBI:** This refers to the AP's Bootloader file.
 - This File Type only supports the Download command. You cannot upload the AP's Bootloader file to a TFTP server.
- **Generic:** This refers to all files associated with the AP's Public Space features. This includes:
 - The Public Space configuration settings file, **current.txt** (the file contains the settings for all of the parameters that correspond to the Nomadix MIB; see [SNMP Management](#) and [Back-up the AP's Configuration Files](#) for details).
 - The **cacert.pem**, **cakey.pem**, and **server.pem** keys for SSL (see [Secure Socket Layer \(SSL\)](#)).
 - The **images.zip** file containing the ICC images (see [Information and Control Console \(ICC\)](#)).
 - The Image and Partner Image for customizing the internal login pages (see [Changing the Login Screen Logos](#)).



NOTE

The Generic files support both Download and Upload operations.

Download Instructions

Follow these steps to send new files to the AP-2500:

1. Launch your TFTP server application (if necessary).
2. Copy the file or files you want to send to the AP to the TFTP server's root directory.
 - If you are using the SolarWinds TFTP program, the root directory is mostly likely *C:\TFTP-Root*.
3. Click **Commands > Download**.
4. Enter the IP address of the computer running the TFTP server application in the **Server IP Address** field.
5. Enter the name of the file that you want to send to the AP in the **File Name** field.
 - Be sure to include the appropriate file extension (for example, you would enter "images.zip" if you wanted to send the AP an updated set of ICC banner images).
 - Updated firmware image files end in ".bin".
6. Select the appropriate file type from the **File Type** drop-down menu (Config, Img, Bspbl, or Generic; see [File Type Overview](#) for details).
7. Select a **File Operation: Download** or **Download & Reboot**.
 - Select **Download** if you have multiple files to send to the AP.
 - Select **Download & Reboot** if downloading a new image file to the AP.
8. Click **OK**.
 - Result: The TFTP operation begins. A new **TFTP Operation Status** window opens.
9. Click **Close** after the TFTP operation is complete.
10. Repeat the above procedure for the remaining files that you want to send to the AP.
11. Reboot the AP (if you did not select **Download & Reboot**).

Upload

Use the **Upload** tab to upload Configuration and image files from the AP-2500 to the TFTP server.

NOTE

The **Download** and **Upload** commands are from the AP's perspective. In other words, to send files to the AP, use the Download command; to obtain files from the AP, use the Upload command.

The TFTP server must be running and configured to point to the directory to which you want to copy the uploaded file. If you don't have a TFTP server installed on your system, install the TFTP server from the ORiNOCO CD. You can either install the TFTP server from the CD Wizard or run **OEM-TFTP-Server.exe** found in the CD's *Xtras/SolarWinds/* sub-directory.

Follow these steps to upload files from the AP-2500 to your TFTP server's root directory:

1. Launch your TFTP server application (if necessary).
2. Click **Commands > Upload**.
3. Enter the IP address of the computer running the TFTP server application in the **Server IP Address** field.
4. Enter the name of the file that you want to send to the TFTP server in the **File Name** field.
 - Be sure to include the appropriate file extension (for example, you would enter "images.zip" if you want to upload the set of ICC banner images from the AP to the TFTP server).
5. Select the appropriate file type from the **File Type** drop-down menu (Config or Generic; see [File Type Overview](#) for details).
6. Click **OK**.
 - Result: The TFTP operation begins. A new **TFTP Operation Status** window opens.
7. Click **Close** after the TFTP operation is complete.
8. Repeat the above procedure for the remaining files that you want to download from the AP to the TFTP server.

NOTE

The AP uploads files to the TFTP server's root directory. If you are using the SolarWinds TFTP program, the root directory is mostly likely *C:\TFTP-Root*.

Figure 7-2 Upload Command Screen

Reboot

Use the **Reboot** tab to save configuration changes (if any) and reset the AP-2500. Entering a value of 0 (zero) causes an immediate reboot. Note that **Reset**, described below, does not save configuration changes.



CAUTION

Rebooting the AP-2500 will cause all users who are currently connected to lose their connection to the network until the AP-2500 has completed the restart process and resumed operation.

Download Upload **Reboot** Reset Help Link

This tab is used to reboot the access point by specifying the number of seconds before the next reboot. The access point reboots immediately by entering a value of zero.

Warning: Rebooting the access point will cause all users who are currently connected to lose their connection to the network until the unit has completed the restart process and resumed operation.

Please enter the time to reboot (seconds)

Reboot

Figure 7-3 Reboot Command Screen

Reset

Use the **Reset** tab to restore the AP-2500 to factory default conditions. The AP-2500 may also be reset from the **RESET** button located on the side of the unit. Since this will reset the Access Point's current IP address, a new IP address must be assigned. Refer to [Recovery Procedures](#) for more information.



CAUTION

Resetting the AP-2500 to its factory default configuration will permanently overwrite all changes that have made to the unit. The AP-2500 will reboot automatically after this command has been issued.

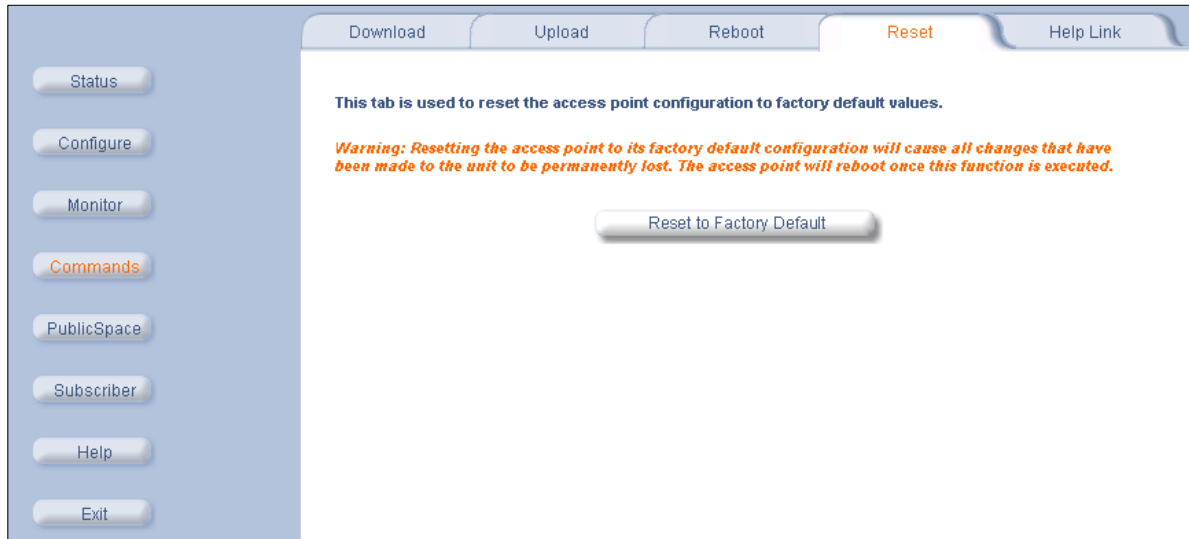


Figure 7-4 Reset to Factory Defaults Command Screen

Help Link

To open **Help**, click the **Help** button on any display screen.

During initialization, the Access Point's on-line help files are downloaded to the default location:

C:\Program Files\ORiNOCO\AP2500\HTML\index.htm.

If you want to place these files on a shared drive, copy the Help Folder to the new location, and then specify the new path in the **Help Link** box.

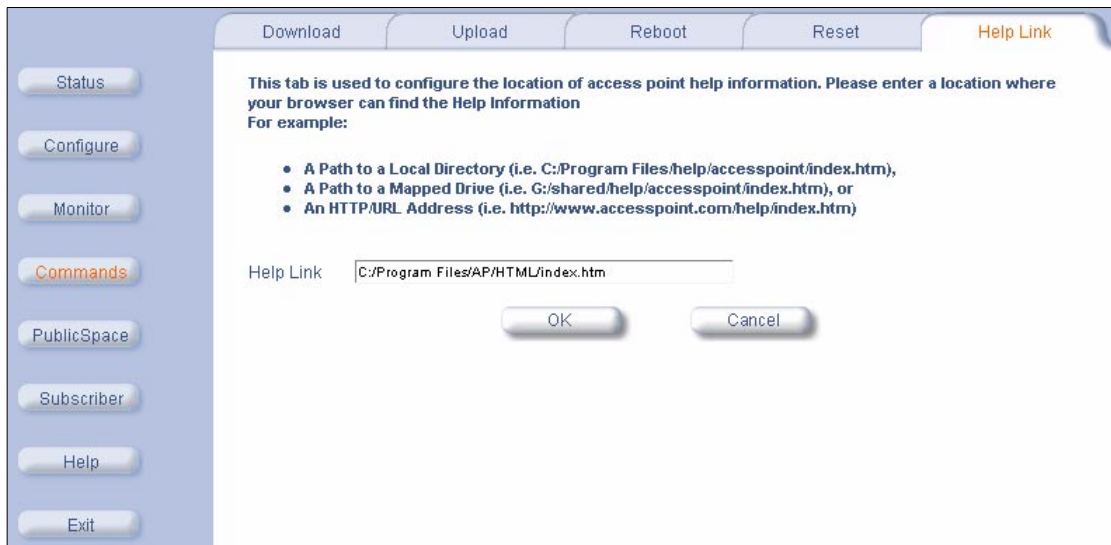


Figure 7-5 Help Link Configuration Screen

8

Troubleshooting

In This Chapter

- Troubleshooting Concepts
- Symptoms and Solutions
 - Connectivity Issues
 - AP-2500 Unit Will Not Boot - No LED Activity
 - Serial Link Does Not Work
 - Ethernet Link Does Not Work
 - Basic Software Setup and Configuration Problems
 - Lost AP-2500, Telnet, or SNMP Password
 - Client Computer Cannot Connect
 - AP-2500 Has Incorrect IP Address
 - HTTP (browser) or Telnet Interface Does Not Work
 - HTML Help Files Do Not Appear
 - Telnet CLI Does Not Work
 - TFTP Server Does Not Work
 - Client Connection Problems
 - Client Manager Finds No Connection
 - Client PC Card Does Not Work
 - Intermittent Loss of Connection
 - Client Does Not Receive an IP Address - Cannot Connect to Internet
 - VLAN Operation Issues
 - Active Ethernet
 - The AP-2500 Unit Does Not Work
 - There Is No Data Link
 - "Overload" Indications
- Recovery Procedures
 - Reset to Factory Default Procedure
 - Forced Reload Procedure
 - Setting IP Address using Serial Port and Normal CLI
- System Alarms (Traps)
 - Security Alarms
 - Wireless Interface Card Alarms
 - Operational Alarms
 - FLASH Memory Alarms
 - TFTP Alarms
 - Image Alarms
 - Standard MIB-II (RFC 1213) Alarms
 - AAA Alarms
- Related Applications
 - RADIUS Server
 - TFTP Server
- LED Indicators

⇒ NOTE

This section helps you locate problems related to the AP-2500 device setup. For details about RADIUS, TFTP, Serial communications program (such as HyperTerminal), Telnet applications or web browsers, please refer to their respective documentation.

Troubleshooting Concepts

The following list identifies important troubleshooting concepts and topics. The most common initialization and installation problems relate to IP Addressing. For example, you must have valid IP Addresses for both the AP-2500 device and the TFTP server before you can transfer files over Ethernet.

- **IP Address management is fundamental.**
- **Factory default units are set for “Dynamic” (DHCP) IP Address assignment.** The default IP Address for the AP-2500 is 10.0.0.10. If you connect the AP-2500 unit to a network with an active DHCP server, then use ScanTool to locate the IP Address of your unit. If a DHCP server is not active on your subnet, then the ScanTool can be used to configure your AP-2500.
- **The Trivial File Transfer Protocol (TFTP) provides a means to download and upload files.** These files include the AP-2500 Image (executable program) and configuration files.
- **If the AP-2500 password is lost or forgotten, you will need to reset to default values.** The [Reset to Factory Default Procedure](#) resets configuration, but does not change the current AP Image.
- **If all else fails...** The [Forced Reload Procedure](#) erases the current AP-2500 Image. Once the new image is loaded, use the [Reset to Factory Default Procedure](#) to set the unit to factory default values and reconfigure the unit.
- **AP-2500 Supports a Command Line Interface (CLI).** If you are having trouble locating your AP-2500 on the network, connect to the unit directly using the serial interface and refer to [Using the Command Line Interface](#) for CLI command syntax and parameter names.

Symptoms and Solutions

Connectivity Issues

Connectivity issues include any issues that prevent you from powering up or connecting to the AP-2500 device.

AP-2500 Unit Will Not Boot - No LED Activity

1. Make sure your power source is operating.
2. Make sure all cables are connected to the AP-2500 unit correctly.
3. With Active Ethernet, make sure you are using a Category 5, foiled, twisted pair cable to power the AP-2500 unit.

Serial Link Does Not Work

1. Make sure you are using the proper serial port cable (a straight-through cable with a 9-pin female connector on each end).
2. Double-check the physical network connections.
3. Make sure your PC terminal program (such as HyperTerminal) is active and configured to the following values:
 - Com Port: (COM1, COM2, etc. depending on your computer);
 - Baud rate: 9600
 - Data bits: 8
 - Stop bits: 1
 - Flow Control: None
 - Parity: None
 - Line Feeds with Carriage Returns
(In HyperTerminal select:
File -> Properties -> Settings -> ASCII Setup -> Send Line Ends with Line Feeds.)

Ethernet Link Does Not Work

1. Double-check the physical network connections. Use a known-good unit to make sure the network connection is present. Once you have the AP-2500 IP Address, you can use the "Ping" command over Ethernet to test the IP Address. If the AP-2500 responds to the Ping, then the Ethernet Interface is working properly.
2. Perform network infrastructure troubleshooting (check switches, routers, etc.).

Basic Software Setup and Configuration Problems

Lost AP-2500, Telnet, or SNMP Password

1. Perform the [Reset to Factory Default Procedure](#) in this guide. This procedure resets system and network parameters, but does not affect the AP-2500 Image.
The default for all AP-2500 passwords is "public".
2. Document your password(s) and store them in a safe location.

Client Computer Cannot Connect

1. Each wireless PC Card in the AP-2500 unit should have a unique Network Name. This Network Name must match the active Network Name on client machines.
2. Network Names should be allocated and maintained by the Network Administrator.

AP-2500 Has Incorrect IP Address

- By default, the AP uses a static IP address of **10.0.0.10**.
- The AP only attempts to contact a DHCP server during boot-up. If you have configured the AP to obtain an IP address from a DHCP server, confirm that the AP is connected to the network before rebooting it. If you do not know the AP's IP address, use ScanTool or the CLI to identify its address.
- To find the current IP Address using DHCP, check the IP Client Table in the DHCP Server to match the AP's MAC Address to its assigned IP address.
- Once you have the current IP Address, use the HTTP or CLI Interface to either set the unit to DHCP mode or assign a static IP Address.
- If you use static IP Address assignments, and cannot access the unit over Ethernet, use the [Initializing the IP Address using Normal CLI](#) procedure. Once the IP Address is set, you can use the Ethernet Interface to complete configuration.
- Perform the [Reset to Factory Default Procedure](#) in this guide. This will reset the unit to "DHCP" mode. If there is a DHCP Server on the same subnet, the DHCP Server will assign an IP Address to the AP-2500.

HTTP (browser) or Telnet Interface Does Not Work

1. Make sure you are using a compatible browser: Microsoft Internet Explorer 5.5 or better (preferred), or Netscape 6 or higher.
2. Make sure you have the proper IP Address. Enter your AP-2500 IP Address in the browser address bar, similar to this example:

http://192.168.1.100

When the AP's **Login** window appears, leave the *User Name* field empty and enter **public** in the *Password* field.

3. Use the CLI over the serial port to check the [IP Access Table](#), which can be restricting access to Telnet and HTTP.

Troubleshooting

HTML Help Files Do Not Appear

1. Verify that the HTML Help files are installed in the default directory listed in the [Help Link](#) screen.
2. If the Help files are not located in this folder, contact your network administrator to find out where the Help files are located on your server.
3. Perform the following steps to verify or enter the pathname for the Help files:
 - a. Click **Commands > Help Link**.
 - b. Enter the path name where the Help files are located.
 - c. Click **OK** when finished.

Telnet CLI Does Not Work

1. Make sure you have the proper IP Address. Enter your AP-2500 IP Address in the Telnet connection dialog, from a DOS prompt, type:

```
C:\> telnet <AP's IP Address>
```
2. Use the CLI over the serial port to check the [IP Access Table](#), which can be restricting access to Telnet and HTTP.

TFTP Server Does Not Work

1. Make sure the TFTP Server has been started.
2. Verify the IP Address of the TFTP Server. The server may be local or remote, so long as it has a valid IP Address.
3. Configure the TFTP Server to “point” to the folder containing the file to be downloaded (or to the folder in which the file is to be uploaded).
4. Verify that you have the proper file names and directory path.

Client Connection Problems

Client Manager Finds No Connection

- Make sure you have configured your client software with the proper Network Name(s). Network Names are typically allocated and maintained by your network administrator.

Client PC Card Does Not Work

1. Make sure you are using the latest PC Card driver software.
2. Download and install the latest client configuration software and driver.

Intermittent Loss of Connection

1. Make sure you are within range of an active AP-2500 device.
2. You can check the signal strength using the client software or the [Link Test \(802.11b Only\)](#).

Client Does Not Receive an IP Address - Cannot Connect to Internet

1. Open the Web-browser interface and select the **Configure** button and then the **Network** tab to make sure the proper DHCP settings are being used.
2. From the client computer, use the “ping” network command to test the connection with the AP-2500 unit. If the AP-2500 device responds, but you still cannot connect to the Internet, there may be a physical network configuration problem (contact your network support staff).
3. For units with Active Ethernet, make sure you are not using a crossover Ethernet cable between the AP-2500 unit and the hub.

VLAN Operation Issues

Verifying Proper Operation of the VLAN Feature

The correct VLAN configuration can be verified by “pinging” both wired and wireless hosts from both sides of the AP-2500 device and the network switch. Traffic can be “sniffed” on both the wired (Ethernet) and wireless (WDS) backbones (if configured). Bridge frames generated by wireless clients and viewed on one of the backbones should contain IEEE 802.1Q compliant VLAN headers or tags. The VLAN ID in the headers should correspond to one of the VLAN User IDs configured for the AP-2500 device.

VLAN Workgroups

The correct VLAN assignment can be verified by pinging the AP-2500 to ensure connectivity, by pinging the switch to ensure VLAN properties, and by pinging hosts past the switch to confirm the switch is functional. Ultimately, traffic can be “sniffed” on the Ethernet or WDS interfaces (if configured) using third-party packages. Most problems can be avoided by ensuring that 802.1Q compliant VLAN tags containing the proper VLAN ID have been inserted in the bridged frames. The VLAN ID in the header should correspond to users assigned network name.

What if network traffic is being directed to a nonexistent host?

- All sessions are disconnected, traffic is lost, and a [Reset to Factory Default Procedure](#) is necessary
- Workaround: you can configure the switch to mimic the nonexistent host



CAUTION

The [Reset to Factory Default Procedure](#) disconnects all users and resets all values to factory defaults.

Active Ethernet

The AP-2500 Unit Does Not Work

1. Verify that you are using a standard UTP Cat. 5 cable, including all 8 wires (4 pairs).
2. Try to move the same load into a different port on the same AE power injector – if it works, there is probably a faulty port or bad RJ-45 port connection.
3. If possible, try to connect the load device into a different AE power injector.
4. Try using a different Ethernet cable – if it works, there is probably a faulty connection over the long cable, or a bad RJ-45 connection.
5. Check power plug and hub.
6. If Ethernet link goes down, check cable, cable type, switch, hub.

There Is No Data Link

1. Verify that the indicator for the port is “on.”
2. Verify that the AE power injector is connected to the Ethernet network with a good connection.
3. Verify that the Ethernet cable is Category 5 or better, and is less than 100 meters (approx. 3.25 ft.) in length from the Ethernet source to the AP-2500.
4. Try to connect a different device over the same port – if it works and link is established, there is probably a faulty data link in the load.
5. Try to re-connect the load into a different output port (remember to move the input port accordingly) – if it works, there is probably a faulty output or input port in the AE power injector or a bad RJ-45 connection.

“Overload” Indications

1. Verify that you are not using any cross-over cable between the AE power injector’s output port to the AP-2500.
2. Verify that there is no short over any of the twisted pair cable or the RJ-45 connector.
3. Move the device into a different output port – if it works, there is probably a faulty port or bad RJ-45 connection.

Recovery Procedures

The most common installation problems relate to IP Addressing. For example, without the TFTP server IP address, you will not be able to download an AP Image to the AP-2500. IP Address management is fundamental. We suggest you create a chart to document and validate the IP addresses for your system.

If the password is lost or forgotten, you will need to reset the AP-2500 to default values. The [Reset to Factory Default Procedure](#) resets configuration settings, but does not change the current AP Image.

If the AP-2500 has a corrupted software image, follow the [Forced Reload Procedure](#) to erase the current AP Image and download a new image.

Reset to Factory Default Procedure

Use this procedure to reset the network configuration values to factory defaults. The current AP Image is not deleted. This procedure may be required if the AP's password is lost or forgotten.

1. Press and hold the **RELOAD** button for about 10 seconds. Result: The AP-2500 reboots, and the factory default network values are restored.
2. Use the ScanTool or normal CLI to set the IP Address. See [Using the Command Line Interface](#) for CLI information.

Forced Reload Procedure

Use this procedure to erase the current AP Image and download a new AP Image. In some cases, specifically when a missing or corrupted AP Image prevents successful booting, you may need to use ScanTool or the Bootloader CLI to download a new executable AP Image.

NOTE

This does not delete the AP's configuration (in other words, the Forced Reload Procedure does not reset to device to factory defaults). If you need to force the AP to the factory default state after loading a new AP image, use the [Reset to Factory Default Procedure](#) above.

For this procedure, you will first erase the AP Image currently installed on the unit and then use either ScanTool or the Bootloader CLI (over the serial port) to set the IP address and download a new AP Image. Follow these steps:

1. While the unit is running, press the **RESET** button.
Result: The AP reboots and the indicators begin to flash.

CAUTION

By completing Step 2, the firmware in the AP will be erased. You will need an Ethernet connection, a TFTP server, and a serial cable (if using the Bootloader CLI) to reload firmware.

2. Press and hold the **RELOAD** button for about 20 seconds until the **POWER LED** turns amber.
Result: The AP deletes the current AP Image.
3. Follow one of the procedures below to load a new AP Image to the Access Point:
 - [Download a New Image Using ScanTool](#)
 - [Download a New Image Using the Bootloader CLI](#)

Download a New Image Using ScanTool

To download the AP Image, you will need an Ethernet connection to the computer on which the TFTP server resides and to a computer that is running ScanTool (this is either two separate computers connected to the same network or a single computer running both programs).

ScanTool detects if an Access Point does not have a valid software image installed. In this case, the **TFTP Server** and **Image File Name** parameters are enabled in the ScanTool's **Change** screen so you can download a new image to the unit. (These fields are grayed out if ScanTool does not detect a software image problem.)

Preparing to Download the AP Image

Before starting, you need to know the Access Point's IP address, subnet mask, the TFTP Server IP Address, and the AP Image file name. Make sure the TFTP server is running and configured to point to the folder containing the image to be downloaded.

Download Procedure

Follow these steps to use ScanTool to download a software image to an Access Point with a missing image:

1. Download the latest software from <http://www.proxim.com/>.
2. Copy the latest software updates to your TFTP server.
3. Launch ScanTool.
4. Highlight the entry for the AP you want to update and click **Change**.
5. Set **IP Address Type** to **Static**.



NOTE

You need to assign static IP information temporarily to the Access Point since its DHCP client functionality is not available when no image is installed on the device.

6. Enter an unused IP address that is valid on your network in the **IP Address** field. You may need to contact your network administrator to get this address.
7. Enter the network's **Subnet Mask** in the field provided.
8. Enter the network's **Gateway IP Address**, if necessary. You may need to contact your network administrator to get this address. You should only need to enter the default gateway address if the Access Point and the TFTP server are separated by a router.
9. Enter the IP address of your TFTP server in the field provided.
10. Enter the **Image File Name** (including the file extension). Enter the full directory path and file name. If the file is located in the default TFTP directory, you need enter only the file name.
11. Click **OK**.
 - Result: The Access Point will reboot and the download will begin automatically. You should see downloading activity begin after a few seconds within the TFTP server's status screen.
12. Click **OK** when prompted that the device has been updated successfully to return to the **Scan List** screen.
13. Click **Cancel** to close the ScanTool.
14. When the download process is complete, reset the AP to factory defaults (see [Reset to Factory Default Procedure](#)) and configure the AP settings or download configuration files to the AP that you saved as a back-up previously.

Download a New Image Using the Bootloader CLI

To download the AP Image, you will need an Ethernet connection to the computer on which the TFTP server resides. This can be any computer on the LAN or connected to the AP with a cross-over Ethernet cable.

You must also connect the AP to a computer with a standard serial cable and use a terminal client, such as HyperTerminal. From the terminal, enter CLI Commands to set the IP address and download an AP Image.

Preparing to Download the AP Image

Before starting, you need to know the Access Point's IP address, subnet mask, the TFTP Server IP Address, and the AP Image file name. Make sure the TFTP server is running and configured to point to the folder containing the image to be downloaded.

Download Procedure

1. Download the latest software from <http://www.proxim.com/>.
2. Copy the latest software updates to your TFTP server's default directory.
3. Use a straight-through serial cable to connect the Access Point's serial port to your computer's serial port.



NOTE

You may need to remove the Access Point's plastic cover to access the serial port.

Troubleshooting

4. Open your terminal emulation program (like HyperTerminal) and set the following connection properties:
 - Com Port: <COM1, COM2, etc., depending on your computer>
 - Baud rate: 9600
 - Data Bits: 8
 - Stop bits: 1
 - Flow Control: None
 - Parity: None
5. Under **File -> Properties -> Settings -> ASCII Setup**, enable the **Send line ends with line feeds** option.
Result: HyperTerminal sends a line return at the end of each line of code.
6. Press the **RESET** button on the AP.
Result: The terminal display shows Power On Self Tests (POST) activity. After approximately 30 seconds, a message indicates: **Sending Traps to SNMP manager periodically**. After this message appears, press the **ENTER** key repeatedly until the following prompt appears:

[Device name]>

7. Enter only the following statements:

```
[Device name]> set ipaddrtype static
[Device name]> set ipaddr <Access Point IP Address>
[Device name]> set ipsubmask <IP Mask>
[Device name]> set tftpipaddr <TFTP Server IP Address>
[Device name]> set tftpfilename <AP Image File Name, including file extension>
[Device name]> set ipgw <Gateway IP Address>
[Device name]> show ip (to confirm your new settings)
[Device name]> show tftp (to confirm your new settings)
[Device name]> reboot 0
```

Example:

```
[Device name]> set ipaddrtype static
[Device name]> set ipaddr 10.0.0.12
[Device name]> set ipsubmask 255.255.255.0
[Device name]> set tftpipaddr 10.0.0.20
[Device name]> set tftpfilename MyImage.bin
[Device name]> set ipgw 10.0.0.30
[Device name]> show ip
[Device name]> show tftp
[Device name]> reboot 0
```

Result: The AP will reboot and then download the image file. You should see downloading activity begin after a few seconds within the TFTP server's status screen.

8. When the download process is complete, reset the AP to factory defaults (see [Reset to Factory Default Procedure](#)) and configure the AP settings or download configuration files to the AP that you saved as a back-up previously.

Setting IP Address using Serial Port and Normal CLI

Use the following procedure to set an IP Address over the serial port using the normal CLI. The network administrator typically provides the AP-2500 IP Address.

Hardware and Software Requirements

- Standard serial data (RS-232) cable with a female DB-9 connector at each end (for newer models) or a standard serial cable and the Mini-DIN8 to DB-9 adapter included in your kit (for older models).
- ASCII Terminal software, such as HyperTerminal.

Attaching the Serial Port Cable

1. Remove power from the AP-2500 and your computer.
2. Connect the serial port cable to the back of the AP-2500 unit and to your computer.
3. Restart the computer and power up the Access Point device.

Initializing the IP Address using Normal CLI

After connecting the serial cable, you may use the CLI to communicate with the AP-2500. You may use most generic terminal programs, such as HyperTerminal. Once the IP Address has been assigned, use the HTTP Interface or the CLI to set the AP's other parameters. Many web sites offer shareware or commercial terminal programs you can download.

Use the following procedure to initialize the AP's IP Address.

1. Open your terminal emulator, and then set the following connection properties:
 - Com Port: <COM1, COM2, etc., depending on your computer>
 - Baud rate: 9600
 - Data Bits: 8
 - Stop bits: 1
 - Flow Control: None
 - Parity: None
2. Enable the "ASCII Setup" settings by selecting "Send line ends with line feeds". Result: HyperTerminal sends a line return at the end of each line of code.
3. Press the **RESET** button on the AP-2500 (located on the LED Indicator side of the unit). Result: The terminal display shows Power On Self Tests (POST) activity, and then displays a CLI prompt, similar to the example below. This process may take several minutes.
[Device name]> **Please enter password:**
4. Enter the password (default is "public"). Result: The terminal displays a welcome message and then the CLI Prompt:
[Device name]>
5. Enter **show ip**. Result: Network parameters appear:
[Device name]> **show ip**

```
[Device Name]> show ip
IP/Network Group Parameters
=====
ipaddr       :      10.0.0.1
ipsubmask    :      255.0.0.0
ipgw         :      10.0.0.1
ipttl        :      64
ipaddrtype   :      static

[Device Name]> _
```

Figure 8-1 Result of "show ip" bootloader CLI command

Troubleshooting

- Change the IP Address and other network values using **set** and **reboot** CLI commands, similar to the example dialog below (use your own IP Address and IP Mask). Result: After each entry the CLI reminds you to reboot; however wait to reboot until all commands have been entered.

```
[Device name]> set ipaddrtype static
[Device name]> set ipaddr <IP Address>
[Device name]> set ipsubmask <IP Mask>
[Device name]> set ipgw <Default Gateway IP Address>
[Device name]> reboot 0
```

- After the AP-2500 reboots, verify the new IP Address by reconnecting, and then entering a **show ip** CLI statement (as in Step 5). Alternatively, you can use the “ping” network command from networked computers to test the new IP Address.
- When the proper IP Address is set, use CLI or the HTTP Interface over the LAN to complete configuration and manage operations.

System Alarms (Traps)

Security Alarms

oriTrapAuthenticationFailure	Wireless Card (A and/or B) incompatible vendor detected
oriTrapUnauthorizedManagerDetected	Wireless Card (A and/or B) firmware download failure detected

Wireless Interface Card Alarms

oriTrapWLCNotPresent	Wireless Card (A and/or B) not present
oriTrapWLCFailure	Wireless Card (A and/or B) general failure
oriTrapWLCRemoval	Wireless Card (A and/or B) removal
oriTrapWLCIncompatibleFirmware	Wireless Card (A and/or B) incompatible firmware detected
oriTrapWLCVoltageDiscrepancy	Wireless Card (A and/or B) voltage discrepancy detected
oriTrapWLCIncompatibleVendor	Wireless Card (A and/or B) incompatible vendor detected
oriTrapWLCFirmwareDownloadFailure	Wireless Card (A and/or B) firmware download failure detected

Operational Alarms

oriTrapWatchDogTimerExpired	Watch Dog Timer has expired
oriTrapRADIUSServerNotResponding	RADIUS Server is not responding or error communicating with RADIUS Server
oriTrapModuleNotInitialized	Module has not been initialized
oriTrapDeviceRebooting	Device is rebooting
oriTrapTaskSuspended	Task suspension has been detected
oriTrapBootPFailed	BootP failure detected (no response from BootP Server)
oriTrapDHCPFailed	DHCP Client failure detected (no response from DHCP server)

FLASH Memory Alarms

oriTrapFlashMemoryEmpty	Flash memory card detected empty
oriTrapFlashMemoryCorrupted	Flash memory data corrupted

TFTP Alarms

oriTrapTFTPFailedOperation	TFTP (upload or download) failure detected
oriTrapTFTPOperationInitiated	TFTP (upload or download) operation initiated
oriTrapTFTPOperationCompleted	TFTP (upload or download) operation completed

Troubleshooting

Image Alarms

oriTrapZeroSizeImage	Zero size image has been downloaded to device
oriTrapInvalidImage	Invalid image has been downloaded to device
oriTrapImageTooLarge	Image downloaded to device is too big
oriTrapIncompatibleImage	Incompatible image has been downloaded to device

Standard MIB-II (RFC 1213) Alarms

coldStart	Device has been cold started
warmStart	Device has been warm started
linkUp	Device Link is up (Ethernet interface is up)
linkDown	Device Link is down (Ethernet interface is down)

AAA Alarms

There are two enterprise traps sent from the Public Space functions:

subCapacityReached	Subscriber capacity reached; subscriber tables full
failedLogin	Failed Login attempt

Related Applications

RADIUS Server

If you have configured the AP's RADIUS settings, make sure your network's RADIUS server is configured and running. Otherwise, clients will not be able to log in. There are several reasons the RADIUS server services might be unavailable, here are two typical things to check.

- Make sure you have the proper RADIUS authentication server information setup configured in the AP-2500. Check the RADIUS server IP Address authentication Port number (default is 1812), and Shared Secret.
- Make sure the AP has been added as a RADIUS server client. Also, if the AP's IP address changes, you will need to update the AP's RADIUS client entry on your RADIUS server with this new address.

TFTP Server

The "Trivial File Transfer Protocol" (TFTP) server allows you to transfer files across a network. You can upload files from the AP-2500 for backup or copying, and you can download the files for configuration and AP Image upgrades. The TFTP software is located on the ORiNOCO AP-2500 Installation CD-ROM.

If a TFTP server is not configured and running, you will not be able to download and upload images and configuration files to/from the AP-2500. Remember that the TFTP server does not have to be local, so long as you have a valid TFTP IP Address. TFTP does not have to be running for AP-2500 operations that do not transfer files.

After the TFTP server is installed:

- Check to see that TFTP is configured to point to the directory containing the files you want to download to the AP.
- Make sure you have the proper TFTP server IP Address, the proper file names, and that the TFTP server is connected.
- **Make sure the TFTP server is configured to both send and receive, with no time-out.**

LED Indicators

POWER	ETHERNET	PC CARD A	PC CARD B	INDICATION
Green	Green flash with data activity	Green flash with data activity	Green flash with data activity	Normal Operation
Amber	n/a (not applicable)	Amber	Amber	Rebooting
Amber	n/a	n/a	n/a	Missing or bad AP Image if amber after reboot
Red	Red	n/a	n/a	Power On Self Test (POST) running
n/a	n/a	Red	Red	PC Card incompatible on indicated interface
n/a	n/a	Red	Red	PC Card failure on indicated interface
Green	n/a	Amber	Amber	Indicated interface in Administrative State
n/a	n/a	Off	Off	PC Card not present

A

Using the Command Line Interface

In This Chapter

This section provides details for the Command Line (CLI) Interface used to manage an AP-2500 device. CLI commands can be used to initialize, configure, and manage network operation of the Access Point.

- CLI commands may be entered in real time through a keyboard, or submitted with CLI scripts.
- The CLI is available through both the Serial Port Interface and the Ethernet Interface.



NOTE

All CLI commands and parameters are case-sensitive.

- [Prerequisite Skills and Knowledge](#)
 - [Notation Conventions](#)
 - [Important Terminology](#)
 - [Navigation and Special Keys](#)
 - [CLI Error Messages](#)
- [Command Line Interface \(CLI\) Variations](#)
 - [Bootloader CLI](#)
- [CLI Command Types](#)
 - [Operational CLI Commands](#)
 - [Parameter Control Commands](#)
- [Using Tables & User Strings](#)
 - [Working with Tables](#)
 - [Using Strings](#)
- [Configuring the AP-2500 Unit using CLI commands](#)
 - [Configuring Objects that Require Reboot](#)
 - ["set" CLI Command](#)
 - ["show" CLI Command](#)
- [Set Basic Configuration Parameters using CLI Commands](#)
 - [Log Into the AP-2500 Unit using HyperTerminal](#)
 - [Log Into the AP-2500 Unit using Telnet](#)
 - [Set Basic Configuration Parameters using CLI Commands](#)
- [Other Network Settings](#)
 - [Change your Wireless Interface Settings](#)
 - [Set Interface Management Services](#)
- [Parameter Tables](#)

Using the Command Line Interface

Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts, network access infrastructures, and client-server relationships. In addition, you should be familiar with software setup procedures for typical network operating systems and servers.

Notation Conventions

- Computer prompts are shown in courier font. For example: [Device name] >
- Information that you input as shown is displayed in bold courier font. For example: [Device name] > **set ipaddr 10.0.0.12**
- The names of keyboard keys, software buttons, and field names are displayed in bold type. For example: Click the **Configure** button
- Screen names are displayed in bold italics. For example, the ***System Status*** screen.

Important Terminology

- Config Files - Database files containing the current Access Point configuration. Configuration items include the IP Address and other network-specific values. Config files may be downloaded to the Access Point or uploaded for backup or troubleshooting.
- Download Vs. Upload - Downloads transfer files to the Access Point. Uploads transfer files from the Access Point. The TFTP server performs file transfers in both directions.
- Group - A logical collection of network parameter information. For example, the System Group is composed of several related parameters. Groups can also contain Tables. All items for a given Group can be displayed with a "show" <Group> CLI Command.
- Image File - The Access Point software executed from RAM. To update an Access Point you typically download a new Image File. This file is often referred to as the "AP Image".
- Parameter - A fundamental network value that can be displayed and may be changeable. For example, the Access Point must have a unique IP Address and the Radio PC Cards must know which channel to use. Change parameters with the CLI set Command, and view them with the CLI show Command
- Table - Tables hold parameters for several related items. For example, you can add several potential managers to the SNMP Table. All items for a given Table can be displayed with a show <Table> CLI Command.
- TFTP - Refers to the TFTP Server, used for file transfers.

Navigation and Special Keys

This CLI supports the following navigation and special key functions to move the cursor along the prompt line.

Key Combination	Operation
Delete or Backspace	Delete previous character
Ctrl-A	Move cursor to beginning of line
Ctrl-E	Move cursor to end of line
Ctrl-F	Move cursor forward one character
Ctrl-B	Move cursor back one character
Ctrl-D	Delete the character the cursor is on
Ctrl-U	Delete all text to left of cursor
Ctrl-P	Go to the previous line in the history buffer
Ctrl-N	Go to the next line in the history buffer
Tab	Complete the command line
?	List available commands

Using the Command Line Interface

CLI Error Messages

The following table describes the error messages associated with improper inputs or expected CLI behavior.

Error Message	Description
% Syntax error	Invalid syntax entered at the command prompt.
% Invalid command	A non-existent command has been entered at the command prompt.
% Invalid parameter name	An invalid parameter name has been entered at the command prompt.
% Invalid parameter value	An invalid parameter value has been entered at the command prompt.
% Invalid table index	An invalid table index has been entered at the command prompt.
% Invalid table parameter	An invalid table parameter has been entered at the command prompt.
% Invalid table parameter value	An invalid table parameter value has been entered at the command prompt.
% Read only parameter	User is attempting to configure a read-only parameter.
% Incorrect password	An incorrect password has been entered in the CLI login prompt.
% Download unsuccessful	The download operation has failed due to incorrect TFTP server IP Address or file name.
% Upload unsuccessful	The upload operation has failed due to incorrect TFTP server IP Address or file name.

Command Line Interface (CLI) Variations

Administrators use the CLI to control Access Point operation and monitor network statistics. The AP-2500 supports two types of CLI: the Bootloader CLI and the normal CLI. The Bootloader CLI provides a limited command set, and is used when the current AP Image is bad or missing. The Bootloader CLI allows you to assign an IP Address and download a new image. Once the image is downloaded and running, the Access Point uses the normal CLI. This guide covers the normal CLI unless otherwise specified.

Bootloader CLI

The Bootloader CLI is a minimal subset of the normal CLI used to perform initial configuration of the AP-2500 device. This interface is only be accessible via the serial interface if the AP-2500 unit does not contain an image (binary) or the TFTP operation has failed as result of the download command for an image.

The Bootloader CLI provides you with the ability to configure the initial setup parameters as well as download an image (binary) to the device.

The Bootloader CLI supports the following functions:

- configuration of initial device parameters using the **set** command
- **show** command to view the device's configuration parameters
- **help** command to provide additional information on all commands supported by the Bootloader CLI
- **reboot** command to reboot the device.

The parameters supported by the Bootloader CLI (for viewing and modifying) are:

- System Name
- IP Address Assignment Type
- IP Address
- IP Mask
- Gateway IP Address
- TFTP Server IP Address
- Image (binary) File Name

Using the Command Line Interface

The following lists display the results of using the **help** and **show** commands in the Bootloader CLI:

[DeviceName] >**help**<CR>

```
[Device name]> help

Command List      Description
=====
set               Set system parameters
show             Show running system information
help             Description of commands, command usage and parameters
reboot           reboot the target

Command Usage
=====
set <parameter name> <parameter value> <cr>
show <cr>
help <cr>
reboot <cr>

Parameter List    Description
=====
sysname           System Name
ipaddr            System IP Address
ipsubmask         System Subnet Mask
ipgw              System Default Gateway IP Address
tftpipaddr        TFTP Server IP Address
tftpfilename       Image or Binary File name
ipaddrtype        System IP Address Type - STATIC or DYNAMIC

[Device name]>
```

Figure A-1 Results of “help” bootloader CLI command

```
[DeviceName] >show<CR>

sysname           <value of sysname>
ipaddrtype        <value of ipaddrtype>
ipaddr            <value of ipaddr>
ipsubmask         <value of ipsubmask>
ipgw              <value of ipgw>
tftpipaddr        <value of tftpipaddr>
tftpfilename       <value of tftpfilename>
```

CLI Command Types

This guide divides CLI Commands into two categories: Operational and Parameter Control.

Operational CLI Commands

This type affects Access Point behavior, such as downloading, rebooting, and so on. After entering commands (and parameters if any) press the Enter key to execute the Command Line.

Operational commands include.

- ? - (Question Mark) Lists CLI Commands or parameters, depending on usage
- done, exit, quit - Terminates the CLI session
- download - Uses TFTP server to download “image”, “config”, “generic”, or “bootloader upgrade” files to the AP
- help - Displays general CLI help information or command help information, such as command usage and syntax
- history - Remembers commands to help avoid re-entering complex statements
- passwd - Sets the Access Point CLI password
- reboot - Reboots the Access Point in specified time
- search - Lists the parameters in a specified Table
- upload - Uses TFTP server to upload “config” or “generic” files from AP to TFTP default directory or specified path

Using the Command Line Interface

? (List Commands)

This command has varied uses to display commands and parameters, depending on the operation in which it is used. The following table lists each operation and provides a basic example. Following the table are detailed examples and display results for each operation.

Operation	Basic Example
Display the Command List (Example 1)	[Device Name] >?
Display commands that start with specified letters (Example 2)	[Device Name] >s?
Display parameters for set and show Commands (Examples 3a and 3b)	[Device Name] >set ? [Device Name] >show ipa?
Prompt to enter successive parameters for Commands (Example 4)	[Device Name] >download?

Example 1. Display Command list

To display the Command List, enter "?"

[Device Name] >?<CR>

```
[Device Name]>
show
set
download
upload
reboot
passwd
help
quit
done
exit
history
search
[Device Name]> _
```

Figure A-2 Result of "?" CLI command

Example 2. Display specific Commands

To show all commands that start with specified letters, enter one or more letters, then "?" with no space between letters and "?".

[Device Name] >s?<CR>

```
[Device Name]> s
show          set          search
```

Figure A-3 Result of "s?" CLI command

Example 3. Display parameters for set and show

Example 3a allows you to see every possible parameter for the set (or show) commands. Notice from example 3a that the list is very long. Example 3b shows how to display a subset of the parameters based on initial parameter letters.

Example 3a. Display every parameter that can be changed

[Device Name] >set?<CR>

Using the Command Line Interface

```
[Wireless LAN AP1]> set
etherspeed
httpifbitmask
httphelplink
httppasswd
httpport
ipaddr
ipaddrtype
iparpfltaddr
iparpfltstatus
iparpfltsubmask
ipgw
ipsubmask
ipttl
mgmtipaccessb1
.
.
.
partnerImageOn
partnerImageFileName
pptpOn
pptpIdleTimeout
ipsecOn
aaaAuthSubTable
aaaSubCurrTable
acIpRangeTable
passthroughDNSTable
passthroughIPTable
urlFilteringIPTable
urlFilteringDNSTable
```

Figure A-4 Result of “set ?” CLI command

Example 3b. Display parameters based on letter sequence

This example shows entries for parameters that start with the letter “i”. The more letters you enter, the fewer the results returned. Notice that there is no space between the letters and the question mark.

[Device Name]> show ipa?<CR>

```
[Device Name]> show ipa
ipaddr      ipaddrtype      iparp
iparpfltaddr iparpfltstatus  iparpfltsubmask
```

Figure A-5 Result of “show ipa?” CLI command

[Device Name]> show iparp?<CR>

```
[Device Name]> show iparp
iparp      iparpfltaddr      iparpfltstatus
iparpfltsubmask
[Device Name]> show iparp_
```

Figure A-6 Result of “show iparp?” CLI command

Example 4. Display Prompts for Successive Parameters

Enter the command, a space, and then “?”. Then, when the parameter prompt appears, enter the parameter value. Result: The parameter is changed and a new CLI line is echoed with the new value (in the first part of the following example, the value is the IP Address of the TFTP server).

Using the Command Line Interface

After entering one parameter, you may add another "?" to the new CLI line see the next parameter prompt, and so on until you enter all parameters. The following example shows how this is used for the "download" Command. The last part of the example shows the completed download Command ready for execution.

```
[Device Name]> download ?  
<TFTP IP Address>  
[Device Name]> download 10.0.0.2 ?  
<File Name>  
[Device Name]> download 10.0.0.2 apimage ?  
<file type (config/img/bootloader/generic)>  
[Device Name]> download 10.0.0.2 apimage img
```

done, exit, quit

Each command disconnects the CLI Session.

```
[Device Name]> done  
[Device Name]> exit  
[Device Name]> quit
```

download

Downloads the specified file from TFTP server to the Access Point. Executing 'download' in combination with the asterisks character, "*", will make use of the previously set TFTP parameters. Executing download without parameters will display command help and usage information. To see a list of available files to download, enter a question mark (?) after download (example: download?).

1. Syntax to download a file:

```
Device Name]>download <tftp server address> <path and filename> <file type>
```

Example:

```
[Device Name]>download 192.168.1.100 MyImage2.bin img
```

2. Syntax to display help and usage information:

```
[Device Name]>download
```

3. Syntax to execute the download Command using previously set (stored) TFTP Parameters:

```
[Device Name]>download *
```

help

Displays instructions on using control-key sequences for navigating a Command Line, and displays command information and examples.

1. Using help as the only argument:

```
[Device Name]>help<space>
```

Using the Command Line Interface

```
[Device Name]> help
Type ? at the command prompt for a command list.

Complete command description and command usage can be provided by:
help <command name> <CR>
<command name> help <CR>

Special keys supported:
Arrow Keys
DEL, BS .... delete previous character
Ctrl-A .... go to beginning of line
Ctrl-E .... go to end of line
Ctrl-F .... go forward one character
Ctrl-B .... go backward one character
Ctrl-D .... delete current character
Ctrl-U, X .. delete to beginning of line
Ctrl-K .... delete to end of line
Ctrl-W .... delete previous word
Ctrl-T .... transpose previous character
Ctrl-P .... go to previous line in history buffer
Ctrl-N .... go to next line in history buffer

Tab .... will attempt command completion
# .... Comment Character
? .... will provide command listing

Examples:
'?' .... list all the supported commands
'sh?' .... list all commands that start with sh
'show ?' .... list all arguments to the show command
'sh<TAB>' .... complete the 'show' command

[Device Name]>
```

Figure A-7 Results of “help<space>” CLI command

2. Complete command description and command usage can be provided by:

```
[Device Name]>help <command name>
[Device Name]><command name> help
```

history

Shows content of Command History Buffer. The Command History Buffer stores command statements entered in the current session. To avoid re-entering long command statements, use the keyboard “up arrow” and “down arrow” keys to recall previous statements from the Command History Buffer. When the desired statement reappears, press the “Enter” key to execute, or you may edit the statement before executing it.

```
[Device Name]> history
```

passwd

Changes the CLI Password.

```
[Device Name]> passwd oldpassword newpassword newpassword
```

reboot

Reboots Access Point after specified number of seconds. Specify a value of 0 (zero) for immediate reboot.

```
[Device Name]> reboot 0
[Device Name]> reboot 30
```

Using the Command Line Interface

search

Lists the members of the specified table. This list corresponds to the table information displayed in the HTTP Interface. In this example, the CLI returns the same table items that are displayed in the HTTP Interface's IP Access Table.

```
[Device Name]> search ?
```

```
[Wireless LAN AP]> search
mgmtipaccesstbl
secenckeylentbl
snmptraphosttbl
stptbl
vlanidtbl
wdstbl
wif
wifsec
aaaAuthSubTable
aaaSubCurrTable
acIpRangeTable
datSessionTable
dhcpLeaseTable
passthroughDNSTable
passthroughIPTable
urlFilteringIPTable
urlFilteringDNSTable
```

```
[Device Name]> search mgmtipaccesstbl
```

```
[Device Name]> search mgmtipaccesstbl
The supported elements are:
index
ipaddr
ipmask
cmt
status
```

Figure A-8 Results of “search” and “search mgmtipaccesstbl” CLI command

upload

Uploads the specified file from AP-2500 to TFTP Server directory. Executing 'upload' with the asterisks, “*”, character will make use of the previously set/stored TFTP parameters. Executing 'upload' without parameters will display command help and usage information.

1. Syntax to upload a file:

```
[Device Name]>upload <tftp server address> <path and filename> <filetype>
```

Example:

```
[Device Name]>upload 192.168.1.100 APImage2 img
```

2. Syntax to display help and usage information:

```
[Device Name]>help upload
```

3. Syntax to execute the upload command using previously set (stored) TFTP Parameters:

```
[Device Name]>upload *
```


Using the Command Line Interface

Parameter Control Commands

The following sections cover each CLI Command, and include several tables showing parameter properties. The two Parameter Control Commands are show and set. These allow you to view (show) all parameters and statistics, and to change (set) parameters.

- **show** - To see any Parameter or Statistic values, you specify a single parameter, a Group, or a Table. For more details, refer to "set and show command examples" later in this guide.
- **set** - Use this CLI Command to change parameter values. You can use a single CLI Statement to modify Tables, or modify each parameter separately. For more details, refer to "set and show command examples" later in this guide.

"set" and "show" Command Examples

In general, you will use the CLI "show" Command to view current parameter values, and use the CLI "set" Command to change parameter values. As shown in the following six examples, parameters may be set individually, and all parameters for a given table can be set with a single statement.

Example 1 - Set the Access Point IP Address Parameter

Syntax:

```
[Device Name]>set <parameter name> <parameter value>
```

Example:

```
[Device Name]> set ipaddr 10.0.0.12
```

Result: IP Address will be changed when you reboot the Access Point. The CLI reminds you when rebooting is required for a change to take effect. To reboot immediately, enter **reboot 0** (zero) at the CLI prompt.

Example 2 - Create a table entry or row

Use 0 (zero) as the index to the table when creating an entry. When creating a table row, only the mandatory table elements are required (comment is usually an optional table element). There are other optional table elements, which, if not entered, the default value applies.

Syntax:

```
[Device Name]>set <table name> <table index> <element 1> <value 1> ...  
                <element n> <value n>
```

Example:

```
[Device Name]> set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0
```

Result: The IP Access Table (Index 0) "IP Address" and "IP Mask" parameters are assigned 10.0.0.10 and 255.255.0.0, respectively.

➡ NOTE

Some tables use a different syntax. See [Working with Tables](#) for details.

Example 3 - Modify a table entry or row

Use the index to be modified and the table elements you would like to modify. For example, suppose the SNMP IP Access table has one entry and you wanted to modify the IP Address:

```
[Device Name]>set mgmtipaccesstbl 1 ipaddr 10.0.0.11
```

You can also modify several elements in the table entry. Enter the index number and specific table elements you would like to modify. Hint: Use the search Command to see the elements that belong to the table.

```
[Device Name]>set mgmtipaccesstbl 1 ipaddr 10.0.0.12 submask 255.255.255.248  
                cmt "First Row"
```

Using the Command Line Interface

⇒ NOTE

Some tables use a different syntax. See [Working with Tables](#) for details.

Example 4 - Enable, Disable, or Delete a table entry or row

In this example you would like to manage the second table row/entry.

Syntax:

```
[Device Name]>set <Table> index status <enable, disable, delete>
[Device Name]>set <Table> index status <1=enable, 2=disable, 3=delete>
```

Example:

```
[Device Name]>set mgmtipaccesstbl 2 status enable
[Device Name]>set mgmtipaccesstbl 2 status disable
[Device Name]>set mgmtipaccesstbl 2 status delete
[Device Name]>set mgmtipaccesstbl 2 status 2
```

⇒ NOTE

You may need to enable a disabled table entry before you can change the entry's elements. Also, some tables use a different syntax. See [Working with Tables](#) for details.

Example 5 - Show the Group Parameters

In this example you can view all elements of a group or table.

Syntax:

```
[Device Name]> show <group name>
```

Example:

```
[Device Name]>show network
```

Result: The CLI displays network group parameters. Note that `show network` and `show ip` work the same.

```
[Device Name]> show network
IP/Network Group Parameters
=====
ipaddr       :      10.0.0.1
ipsubmask    :      255.0.0.0
ipgw         :      10.0.0.1
ipttl        :      64
ipaddrtype   :      static

[Device Name]> show ip
IP/Network Group Parameters
=====
ipaddr       :      10.0.0.1
ipsubmask    :      255.0.0.0
ipgw         :      10.0.0.1
ipttl        :      64
ipaddrtype   :      static

[Device Name]> _
```

Figure A-9 Results of “show network” and “show ip” CLI Commands

Using the Command Line Interface

Example 6 - Show Individual and Table Parameters

1. View a single parameter

Syntax:

```
[Device Name]>show <parameter name>
```

Example:

```
[Device Name]> show ipaddr
```

Result: Displays the Access Point IP Address.

```
[Device Name]> show ipaddr
ipaddr
10.0.0.1
[Device Name]> _
```

Figure A-10 Result of “show ipaddr” CLI Command

2. View all parameters in a table

Syntax:

```
[Device Name]> show <table name>
```

Example:

```
[Device Name]> show mgmtipaccesstbl
```

Result: Displays the IP Access Table and its entries.

Using Tables & User Strings

Working with Tables

Each member of the table must be specified, as in the example below.

```
[Device Name]>set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0
```

The following are the rules for creating, modifying, enabling/disabling, and deleting table entries for the first table syntax.

- Creation
 - The table name is required.
 - The table index is required – for some tables (such as mgmtipaccesstbl), to create an instance the index is always zero (0). For other tables (such as secenckeylentbl), you need to specify the index number.
 - The order in which the table arguments or objects are entered is not important.
 - Parameters that are not required can be omitted, in which case they will be assigned the default value as specified in the MIB or product functional specification document.
- Modification
 - The table name is required.
 - The table index is required – for table modification the index should be the index of the entry to be modified.
 - Only the table objects that are to be modified need to be specified. Not all the table objects are required.
 - If multiple table objects are to be modified the order in which they are entered is not important.
 - If the entire table entry is to be modified, all the table objects have to be specified.
- Enabling/Disabling
 - The table name is required.
 - The table index is required – for table enabling/disabling the index should be the index of the entry to be enabled/disabled.
 - The reserved word enable or disable are required.

Using the Command Line Interface

- Deletion
 - The table name is required.
 - The table index is required – for table deletion the index should be the index of the entry to be deleted.
 - The reserved word delete or destroy is required.

There are some differences between table entry add and delete operations among the available tables.

The following tables use **enable (1)**, **disable (2)**, and **delete (3)** to change an entry's status:

- mgmtipaccesstbl
- secenckeylentbl
- snmptraphosttbl
- wdstbl

The following tables use **createAndGo (4)** to add a row, **active (1)** to enable a row, and **destroy (6)** to delete a row (other Status options for these tables include **notInService (2)**, **notReady (3)**, and **createAndWait (5)**):

- aaaAuthSubTable
- aaaSubCurrTable
- aclpRangeTable
- datSessionTable
- dhcpLeaseTable
- passthroughDNSTable
- passthroughIPTable
- urlFilteringIPTable
- urlFilteringDNSTable

In the following example, a new entry (index 1) is added to the Passthrough IP Table:

```
[Device Name]> set passthroughIPTable 1 passthroughIPTableAddress 123.33.11.1
passthroughIPTableStatus 4
```

Using Strings

Since there are several string objects supported by the AP-2500 device, a string delimiter is required for the strings to be interpreted correctly by the command line parser. For this CLI implementation, the single quote or double quote character can be used at the beginning and at the end of the string.

For example:

```
[Device Name]> set sysname Lobby - Does not need quote marks
[Device Name]> set sysname "Front Lobby" - Requires quote marks.
```

The scenarios supported by this CLI are:

"My Desk in Nieuwegein"	Double Quotes
'My Desk in Nieuwegein'	Single Quotes
"My 'Desk' in Nieuwegein"	Single Quotes within Double Quotes
'My "Desk" in Nieuwegein'	Double Quotes within Single Quotes
"Daniel's Desk in Nieuwegein"	One Single Quote within Double Quotes
'Daniel"s Desk in Nieuwegein'	One Double Quote within Single Quotes

The string delimiter does not have to be used for every string object. The single quote or double quote only has to be used for string objects that contain blank space characters. If the string object being used does not contain blank spaces, then the string delimiters, single or double quotes, mentioned in this section are not required.

Using the Command Line Interface

Configuring Objects that Require Reboot

Certain objects supported by the AP require the device to be rebooted in order for the changes to take effect. In order to inform the end-user of this behavior, the CLI shall provide informational messages when the user has configured an object or object(s) that requires the device to be rebooted. The following message shall be displayed as a result of the configuring such object or objects.

Example 1: Configuring objects that require the device to be rebooted

The following message is displayed every time the user has configured an object that requires the device to be rebooted.

```
[Device Name]>set ipaddr 135.114.73.10  
In order for this change to take effect, the device is required to be rebooted.
```

Example 2: Executing the exit, quit, or done commands when an object that requires reboot has been configured

In addition to the above informational message, the CLI also provides a message as a result of the exit, quit, or done command if changes have been made to objects that require reboot. If you make changes to objects that require reboot and execute the exit command the following message is displayed:

```
[Device Name]>exit<CR> OR quit<CR> OR done<CR>  
Modifications have been made to parameters that require the device to be rebooted. These changes will only take effect after the next reboot.
```

"set" CLI Command

Sets (modifies) the value of given parameter. To see a definition and syntax example, type only set and then press the Enter key. To see a list of available parameters, enter a space, then a question mark (?) after set (example: set?).

Syntax:

```
[Device Name]>set <parameter> <value>  
[Device Name]>set <table> <index> <argument 1> <value 1> ... <argument N> <value N>
```

Example:

```
[Device Name]>set sysloc "Main Lobby"  
[Device Name]>set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0
```

"show" CLI Command

Displays the value of specified parameter, or displays all parameter values of a specified group (parameter table). Groups contain Parameters and Tables. Tables contain parameters for a series of similar entities.

To see a definition and syntax example, type only show and then press the Enter key. To see a list of available parameters, enter a question mark (?) after show (example: show ?).

Syntax:

```
[Device Name]>show <parameter>  
[Device Name]>show <group>  
[Device Name]>show <table>
```

Examples:

```
[Device Name]>show ipaddr  
[Device Name]>show network  
[Device Name]>show mgmtipaccesstbl
```

Using the Command Line Interface

Configuring the AP-2500 Unit using CLI commands

Log Into the AP-2500 Unit using HyperTerminal

1. Launch HyperTerminal from the **Start > Programs** menu. Open an existing connection or create a new one with the following settings:
 - Com Port: <COM1, COM2, etc., depending on your computer>
 - Baud rate: 9600
 - Data Bits: 8
 - Stop bits: 1
 - Flow Control: None
 - Parity: None
2. Enable the "ASCII Setup" settings by selecting "**Send line ends with line feeds**".
(Result: HyperTerminal sends a line return at the end of each line of code.)
3. Enter the Telnet password (default is `public`).



NOTE

Proxim recommends changing your default passwords immediately. To perform this operation using CLI commands, refer to [Change Passwords](#).

Log Into the AP-2500 Unit using Telnet

The CLI commands can be used to access, configure, and manage your AP-2500 device using Telnet or a terminal emulation application, such as HyperTerminal. Log into the AP-2500 unit using Telnet:

1. Go to the DOS command prompt on your computer.
2. Type in `telnet <IP Address of the unit>`.
3. Enter the Telnet password (default is `public`).



NOTE

Proxim recommends changing your default passwords immediately. To perform this operation using CLI commands, refer to [Change Passwords](#).

Set Basic Configuration Parameters using CLI Commands

There are a few basic configuration parameters that you will want to setup right away when you receive the AP-2500 unit. For example:

- [Set System Name, Location and Contact Information](#)
- [Set Static IP Address for the AP-2500 device](#)
- [Set a Network Name for each Wireless Interface](#)
- [Set WEP Encryption for each Wireless Interface](#)
- [Change Passwords](#) for the different management interfaces (SNMP, Telnet, HTTP)

Set System Name, Location and Contact Information

```
[Device Name]>set sysname <system name>
[Device Name]>set sysloc <Unit Location>
[Device Name]>set sysctname <Contact Name (person responsible for system)>
[Device Name]>set sysctphone <Contact Phone Number>
[Device Name]>set systemail <Contact E-mail address>
[Device Name]>show system<CR>
```

Using the Command Line Interface

```
[Device Name]> show system
System Parameters
=====

sysname           :      Device Name
sysloc            :      System Location
sysctname         :      Contact Name
sysctemail        :      name@organization.com
sysctphone        :      Contact Phone Number
sysuptime <DD:HH:MM:SS> :      0:11: 6:40
sysoid            :      1.3.6.1.4.1.11898.2.4.6
sysdescr          :      AP v2.1.0 SN-02UT16570004 v2.0.10
syssservices      :      2
sysflashupdate    :      0
sysflashbckint    :      120
sysresetdefaults  :      0

[Device Name]> _
```

Figure A-11 Result of “show system” CLI Command

Set Static IP Address for the AP-2500 device

```
[Device Name]>set ipaddrtype static
[Device Name]>set ipaddr <fixed IP address of unit>
[Device Name]>set ipsubmask <IP Mask (default = 255.0.0.0)>
[Device Name]>set ipgw <gateway IP address (default = 10.0.0.1)>
[Device Name]>show network<CR>
```

➡ NOTE

The IP Mask of the AP-2500 unit needs to match the IP Mask of your network.

Set a Network Name for each Wireless Interface

- 3 = wireless card in Slot A
- 4 = wireless card in Slot B

```
[Device Name]>set wif 3 netname <Network Name (SSID) for wireless card in Slot A>
[Device Name]>set wif 4 netname <Network Name (SSID) for wireless card in Slot B>
[Device Name]>show wif<CR>
```

Using the Command Line Interface

```
[Device Name]> show wif
Wireless Interface Table
=====
Index                :      3
Network Name         :      My Wireless Network A
Distance Between APs :      large
Interference Robustness :      disable
DTIM Period          :      1
Automatic Channel Selection :      enable
Frequency Channel     :      56
RTS/CTS Medium Reservation :      2347
Multicast Rate        :      2 Mbps
Closed System         :      Not Supported
Load Balancing         :      Not Supported
Medium Density Distribution :      Not Supported
MAC Address           :      00:30:F1:5B:11:0A
Supported Data Rates  :      6 9 12 18 24 36 48 54
Supported Frequency Channels :      52 56 60 64 36 40 44 48
Physical Layer Type   :      OFDM
Regulatory Domain List :      USA <FCC>
Transmit Rate         :      0
TurboMode             :      disable

Index                :      4
Network Name         :      My Wireless Network B
Distance Between APs :      large
Interference Robustness :      disable
DTIM Period          :      1
Automatic Channel Selection :      enable
Frequency Channel     :      11
RTS/CTS Medium Reservation :      2347
Multicast Rate        :      2 Mbps
Closed System         :      disable
Load Balancing         :      enable
Medium Density Distribution :      enable
MAC Address           :      00:02:2D:4C:27:3B
Supported Data Rates  :      1 2 5.5 11
Supported Frequency Channels :      1 2 3 4 5 6 7 8 9 10 11
Physical Layer Type   :      DSSS
Regulatory Domain List :      USA <FCC>
Transmit Rate         :      0
TurboMode             :      disable
```

Figure A-12 Results of “show wif” CLI command

Set WEP Encryption for each Wireless Interface

- 3 = wireless card in Slot A
- 4 = wireless card in Slot B



CAUTION

Client stations must have the same encryption key to be able to communicate with the AP-2500 device. Each Wireless Interface can only support one Key Length (so each of the configured keys must have the same length). The available key sizes vary based on card type. See [Encryption](#) for more information.

For the wireless card in Slot A

You can set up to four encryption keys. This example describes setting encryption Key 1 on the wireless card in Slot A.

```
[Device Name]> set wifsec 3 encrypt enable encryptkey 1
<WEP key (5-13 characters long depending on card type)> encryptkeytx 1
[Device Name]> show wifsec<CR>
```


Using the Command Line Interface

For the wireless card in Slot B

You can set up to four encryption keys. This example describes setting encryption Key 2 on the wireless card in Slot B.

```
[Device Name]>set wifsec 4 encrypt enable encryptkey 2
<WEP key (5-13 characters long depending on card type)> encryptkeytx 2
[Device Name]>show wifsec<CR>
```

```
[Device Name]> show wifsec
Wireless Security table
=====
Index          :          3
EnableEncryption :      disable
EncryptionKey1  :      *****
EncryptionKey2  :      *****
EncryptionKey3  :      *****
EncryptionKey4  :      *****
Encryption Key in Use :      key1
Deny Non Encrypted Data :      enable

Index          :          4
EnableEncryption :      disable
EncryptionKey1  :      *****
EncryptionKey2  :      *****
EncryptionKey3  :      *****
EncryptionKey4  :      *****
Encryption Key in Use :      key1
Deny Non Encrypted Data :      enable
```

Figure A-13 Result of “show wifsec” CLI Command

Change Passwords

```
[Device Name]>passwd <old password> <new password> <confirm password> (CLI password)
[Device Name]>set httppasswd <new password>
[Device Name]>set snmprpasswd <new password> (SNMP read password)
[Device Name]>set snmprpasswd <new password> (SNMP read/write password)
[Device Name]>reboot 0
```



CAUTION

Proxim strongly urges you to change the default passwords to restrict access to your network devices to authorized personnel. If you lose or forget your password settings, you can always perform the [Reset to Factory Default Procedure](#).

Other Network Settings

There are other configuration settings that you may want to set for your AP-2500 unit. Examples are provided below.

- [VLAN Management](#)
- [Change your Wireless Interface Settings](#)
- [Set Interface Management Services](#)

VLAN Management

Add Entry to VLAN ID Table

- 3 = wireless card in Slot A
- 4 = wireless card in Slot B

```
[Device Name]>set vlanidtbl <index (1 or 2)> id <0 (disable) o 1-4094>
[Device Name]>reboot 0
[Device Name]>show vlanidtbl
```

Using the Command Line Interface

Change your Wireless Interface Settings

Enable/Disable Interference Robustness

- 3 = wireless card in Slot A
- 4 = wireless card in Slot B

[Device Name]>**set wif** <3 or 4> **interrobust** <enable/disable>

This feature is only available for 802.11b wireless cards.

Enable/Disable Closed System

- 3 = wireless card in Slot A
- 4 = wireless card in Slot B

[Device Name]>**set wif** <3 or 4> **closedsys** <enable/disable>

⇒ NOTE

When disabled, a client configured with the Network Name "ANY" can connect to the AP-2500. This feature is only available for 802.11b wireless cards.

Enable/Disable Load Balancing

- 3 = wireless card in Slot A
- 4 = wireless card in Slot B

[Device Name]>**set wif** <3 or 4> **ldbalance** <enable/disable>

This feature is only available for 802.11b wireless cards.

Enable/Disable Medium Density Distribution

- 3 = wireless card in Slot A
- 4 = wireless card in Slot B

[Device Name]>**set wif** <3 or 4> **meddendistrib** <enable/disable>

This feature is only available for 802.11b wireless cards.

Autochannel Select (ACS)

ACS is enabled by default. In order to disable ACS, disable the cards in slots A and B and reboot.

- 3 = wireless card in Slot A
- 4 = wireless card in Slot B

[Device Name]>**set wif** <3 or 4> **autochannel** **disable**

[Device Name]>**reboot** 0

Re-enable ACS

- 3 = wireless card in Slot A
- 4 = wireless card in Slot B

[Device Name]>**set wif** <3 or 4> **autochannel** **enable**

[Device Name]>**reboot** 0

Set the Distance Between APs

- 3 = wireless card in Slot A
- 4 = wireless card in Slot B

[Device Name]>**set distaps** <large, medium, small, minicell, microcell>

[Device Name]>**reboot** 0

This feature is only available for 802.11b wireless cards.

Using the Command Line Interface

⇒ NOTE

The distance between APs should not be approximated. It is calculated by means of a manual Site Survey, in which an AP-2500 unit is set up and clients are tested throughout the area to determine signal strength and coverage, and local limits such as physical interference are investigated. From these measurements the appropriate cell size and density is determined, and the optimum distance between APs is calculated to suit your particular business requirements.

Set the Multicast Rate

⇒ NOTE

The Distance Between APs **must be set before** the Multicast Rate.

- 3 = wireless card in Slot A
- 4 = wireless card in Slot B

```
[Device Name]>set wif <3 or 4> multrate <1,2,5.5,11 (Mbps)>
```

This feature is only available for 802.11b wireless cards.

Set Ethernet Speed and Transmission Mode

```
[Device Name]>set etherspeed <value (see below)>
```

```
[Device Name]>reboot 0
```

Ethernet Speed and Transmission Mode	Value
10 Mbit/s - half duplex	10halfduplex
10 Mbit/s - full duplex	10fullduplex
10 Mbit/s - auto duplex	10autoduplex
100 Mbit/s - half duplex	100halfduplex
100 Mbit/s - full duplex	100fullduplex
Auto Speed - half duplex	autohalfduplex
Auto Speed - auto duplex	autoautoduplex (recommended)

Set Interface Management Services

Set Communication Ports

```
[Device Name]>set httpport <HTTP port number (default is 80)>
```

```
[Device Name]>set telport <Telnet port number (default is 23)>
```

Set Session Timeouts

```
[Device Name]>set tellogintout <time in seconds>
```

```
[Device Name]>set telsessiontout <time in seconds>
```

Using the Command Line Interface

Configure Management Ports

```
[Device Name]>set snmpifbitmask <0, 1, 4, 8, 15 (see below)>
[Device Name]>set httpifbitmask <0, 1, 4, 8, 15 (see below)>
[Device Name]>set telifbitmask <0, 1, 4, 8, 15 (see below)>
```

Choose from the following values:

Interface bitmask	Description
0 = disable (all interfaces)	All management channels disabled
1 = ethernet if	Ethernet only enabled
4 = pcCardA if	Wireless A only enabled
8 = pcCardB if	Wireless B only enabled
15 = allInterfaces	All management channels enabled

Edit IP Access Table

```
[Device Name]>set mgmtipaccesstbl <index> ipaddr <IP address> ipmask <subnet mask>
```

Configure Serial Port Interface

```
[Device Name]>set serbaudrate <2400, 4800, 9600, 19200, 38400, 57600>
[Device Name]>set serflowctrl <none, xon/xoff>
[Device Name]>show serial
```

```
[Device Name]> show serial
Serial Interface Group Parameters
=====
serbaudrate           :      9600
serdatabits           :          8
serparity             :      none
serstopbits           :          1
serflowctrl           :      none
```

Figure A-14 Result of “show serial” CLI Command

➤ NOTE

To avoid unexpected performance of your AP-2500, leave the setting Flow Control to its default value (none) unless you are sure what this setting should be.

Using the Command Line Interface

Parameter Tables

Objects contain groups that contain both parameters and parameter tables.

Use the following Tables to configure the Access Point. The Access Point CLI is under development as this document is being prepared; therefore, some table cells are blank where a feature has not yet been implemented or information needs validation. Columns used on the tables include:

- Name - Parameter, Group, or Table Name
- Type - Data type
- Values - Value range, and default value, if any
- ACC. - Indicates access type. R = Read Only (show), RW = Read-Write, can be "set", W = Write Only
- CLI Parameter - Parameter name as used in the Access Point

Access Point network objects are associated with Groups. The network objects are listed below and associated parameters are described in the following Parameter Tables:

- [System Parameters](#) - Access Point system information
 - [Miscellaneous System Parameters](#)
 - [Inventory Management Information](#)
- [Network Parameters](#) - IP, DHCP, DNS and VLAN configuration
 - [DHCP Server Parameters](#)
 - [DNS Parameters](#)
 - [VLAN Parameters](#)
- [Interface Parameters](#) - Wireless and Ethernet configuration
 - [Wireless 802.11b Parameters](#) (including WDS)
 - [Wireless 802.11a Parameters](#)
 - [Ethernet Interface Parameters](#)
- [Management Parameters](#) - Control access to the AP-2500's management interfaces and set the time
 - [SNMP Parameters](#)
 - [SNMP Table Host Table Parameters](#)
 - [Telnet Parameters](#)
 - [Serial Port Parameters](#)
 - [HTTP \(web browser\) Parameters](#)
 - [TFTP Server Parameters](#)
 - [NTP Parameters](#)
- [Security Parameters](#) - Access Point security settings and RADIUS configuration
 - [RADIUS Server Parameters](#)
 - [Encryption Parameters](#)
 - [VPN](#)
- [AAA Parameters](#) - Configure Authentication, Authorization and Accounting (AAA) settings
 - [Basic AAA Parameters](#)
 - [AAA External Authorization Parameters](#)
 - [AAA Internal Authorization Parameters](#)
- [Logging Parameters](#) - System and AAA Logging
- [URL Filtering Parameters](#) - Prevent subscribers from accessing specified Web sites
 - [URL Filtering IP Table](#)
 - [URL Filtering DNS Table](#)
- [ICC \(Information Control Console\) Parameters](#) - Configure the Information and Control Console
 - [ICC Button Configuration](#)
 - [ICC Banner Configuration](#)
- [SMTP Parameters](#) - Enable redirection of outgoing e-mails

Using the Command Line Interface

- [Passthrough Parameters](#) - Specify free content or walled garden sites for unauthenticated users
 - [Passthrough IP Table](#)
 - [Passthrough DNS Table](#)
 - [AAA Passthrough Port](#)
- [Bandwidth Management Parameters](#) - Enable bandwidth management control for subscribers
- [Billing Parameters](#) - Configure billing plans and bill mirroring for internal authentication
 - [Billing Mirroring Parameters](#)
 - [Billing Plans Configuration](#)
- [Subscriber Messages Parameters](#) - Configure the user interface presented to subscribers by internal web server
- [Authorized Subscribers Table](#) - Manage list of authorized subscribers
- [Current Subscribers Table](#) - View list of subscribers associated with AP
- [Miscellaneous Parameters](#) - Set VPN parameters and partner image for connecting page
- [CLI Monitoring Parameters](#) - View AP-2500's statistics

System Parameters

Name	Type	Values	Access	CLI Parameter
System	Group	N/A	R	system
Name	DisplayString	User Defined	RW	sysname
Location	DisplayString	User Defined	RW	sysloc
Contact Name	DisplayString	User Defined	RW	sysctname
Contact E-mail	DisplayString	User Defined	RW	sysctemail
Contact Phone	DisplayString	User Defined max 254 characters	RW	sysctphone
FLASH Backup Interval	Integer	0 - 65535 seconds	RW	sysflashbckint
Flash Update		0 1	RW	sysflashupdate
System OID	DisplayString	N/A	R	sysoid
Descriptor	DisplayString	System Name, flash version, S/N, bootloader version	R	sysdescr
Up Time	Integer	dd:hh:mm:ss dd – days hh – hours mm – minutes ss – seconds	R	sysuptime
Emergency Restore to defaults		Resets all parameters to default factory values	RW	sysresettodefaults Note: You must enter the following command twice to reset to defaults: set sysresettodefaults 1

Miscellaneous System Parameters

Name	Type	Values	Access	CLI Parameter
NSE System	Group	N/A	R	nse
System Date and Time	DisplayString Size(20..24)	N/A	R	systemCurrentDateAndTime
System Unit ID Number	DisplayString Size(1..32)	N/A	R	systemUsGId
Bridge Mode	Integer	disable (0) enable (1)	RW	systemBridgeMode
System Version	DisplayString Size(1..32)	N/A	R	systemVersion
SNMP Version	DisplayString Size(1..32)	N/A	R	snmpVersion
SSL Version	DisplayString Size(1..32)	N/A	R	sslVersion

Using the Command Line Interface

Inventory Management Information

Name	Type	Values	Access	CLI Parameter
System Inventory Management	Subgroup	N/A	R	sysinvmgmt
Component Table	Subgroup	N/A	R	sysinvmgmtcmptbl
Component Interface Table	Subgroup	N/A	R	sysinvmgmtcmpiftbl

NOTE

The inventory management commands display advanced information about the AP's installed components. You may be asked to report this information to a technical representative if you contact customer support.

Network Parameters

Name	Type	Values	Access	CLI Parameter
Network	Group	N/A	R	network
IP Configuration	Group	N/A	R	ip (Note: The network and ip parameters display the same information)
IP Address	IpAddress	User Defined	RW	ipaddr
IP Mask	IpAddress	User Defined	RW	ipmask
Default Router IP Address	IpAddress	User Defined	RW	ipgw
Default TTL	Integer	User Defined 64 (default)	RW	ipttl
Address Type	Integer	static dynamic (default)	RW	ipaddrtype

NOTE

The IP Address Assignment Type (ipaddrtype) must be set to static before the IP Address (ipaddr), IP Mask (ipsubmask) or Default Gateway IP Address (ipgw) values can be entered.

Location Parameters

You can also configure the AP's basic IP settings using the following Location parameters:

Name	Type	Values	Access	CLI Parameter
Location	Group	N/A	R	location
Network IP Address	IpAddress	User Defined	RW/Reboot	locationNetworkIp
Network Subnet Mask	DisplayString Size(0..238)	User Defined	RW/Reboot	locationNetmask
Gateway IP Address	IpAddress	User Defined	RW/Reboot	locationGateway

Using the Command Line Interface

DHCP Server Parameters

Name	Type	Values	Access	CLI Parameter
DHCP	Group	N/A	R	dhcp
DHCP Service	Integer	disable (0) enable (1)	RW/Reboot	dhcpDisable
DHCP IP Upsell Service	Integer	disable (0) enable (1)	RW/Reboot	dhcpIpUpsell
DHCP Server Service	Integer	disable (0) enable (1)	RW/Reboot	dhcpServerEnable
DHCP IP Pool Public	Integer	private (0) public (1)	RW/Reboot	dhcpServerPublic
DHCP Server IP	IpAddress	User Defined	RW/Reboot	dhcpServerIP
DHCP Server Subnet Mask	IpAddress	User Defined	RW/Reboot	dhcpServerNetmask
DHCP Lease Pool IP Start	IpAddress	User Defined	RW/Reboot	dhcpPoolStartIP
DHCP Lease Pool IP Stop	IpAddress	User Defined	RW/Reboot	dhcpPoolStopIP
DHCP Lease Duration	Integer	0..65536	RW/Reboot	dhcpLeaseMinutes
DHCP Relay Service	Integer	disable (0) enable (1)	RW/Reboot	dhcpRelayEnable
DHCP Relay Public	Integer	private (0) public (1)	RW/Reboot	dhcpRelayPublic
DHCP Relay Agent IP	IpAddress	User Defined	RW/Reboot	dhcpRelayAgentIP
DHCP Relay Server IP	IpAddress	User Defined	RW/Reboot	dhcpRelayServerIP
DHCP Lease Table	Table	N/A	R	dhcpLeaseTable
Lease Table Index	Counter	N/A	R	leaseIndex
IP Address	IpAddress	N/A	R	leaseAddress
Client ID	MacAddress	N/A	R	leaseCLID
Lease Status	Integer	available (0), reserved (1)	R	leaseStatus

DNS Parameters

Name	Type	Values	Access	CLI Parameter
DNS	Group	N/A	R	dns
DNS Host Name	DisplayString Size(1..32)	User Defined	RW/Reboot	dnsHostName
DNS Domain	DisplayString Size(1..32)	User Defined	RW/Reboot	dnsDomain
Primary DNS Server	IpAddress	User Defined	RW/Reboot	dnsPrimaryServer
Secondary DNS Server	IpAddress	User Defined	RW/Reboot	dnsSecondaryServer
Tertiary DNS Server	IpAddress	User Defined	RW/Reboot	dnsTertiaryServer

Using the Command Line Interface

VLAN Parameters

Name	Type	Values	Access	CLI Parameter
VLAN	Group	N/A	R	vlan
Status	Integer	enable disable (default)	RW	vlanstatus

VLAN ID Table

Name	Type	Values	Access	CLI Parameter
VLAN ID Table	Table	N/A	R	vlanidtbl
Index	Integer32	1 (Wireless A) 2 (Wireless B)	R	index
Identifier (ID)	Vlanid	0 (disable) or 1 – 4094	RW	id

Interface Parameters

Since the AP-2500 devices support two PC Card slots, we differentiate the two wireless interfaces by using the table index:

- Slot A = index 3
- Slot B = index 4

The wireless interface group parameter is **wif**, which displays the objects associated with both PC Cards A and B.

Wireless 802.11b Parameters

Name	Type	Values	Access	CLI Parameter
Wireless Interfaces	Group	N/A	R	wif
Network Name	DisplayString	1 – 31 characters My Wireless Network A (default) My Wireless Network B (default)	RW	netname
Distance between APs	Integer	large (default) medium small minicell microcell	RW	distaps
Auto Channel Select (ACS)	Integer	enable (default) disable	RW	autochannel
Interference Robustness	Integer	enable (default) disable	RW	interrobust
DTIM Period	Integer	1 – 65535 1 = default	RW	dtimperiod
Operating Frequency Channel	Integer	1 - 11 (FCC) (3 = default) 1 - 13 (ETSI) (3 = default) 1 - 14 (JP) (3 = default) 10 - 13 (FR) (10 = default)	RW	channel
RTS/CTS Medium Reservation	Integer	0 – 2347 Default is 2347 (off)	RW	medres
Multicast Rate	Integer	1 Mbit/sec (1) 2 Mbit/sec (2) (default) 5.5 Mbit/sec (3) 11 Mbit/sec (4)	RW	multirate
Closed Wireless System	Integer	enable disable (default)	RW	closedsys
Load Balancing	Integer	enable (default) disable	RW	ldbalance

Using the Command Line Interface

Name	Type	Values	Access	CLI Parameter
Medium Distribution	Integer	enable (default) disable	RW	meddendistrib
MAC Address	PhyAddress	12 hex digits	R	macaddr
Supported Data Rates	Octet String	Reported in 500 Kb/sec intervals: 2 (1 Mbit/sec) 4 (2 Mbit/sec) (default) 11 (5.5 Mbit/sec) 22 (11 Mbit/sec)	R	suppdatarates
Transmit Rate	Integer32	Reported in 500 Kb/sec intervals: 0 (auto fallback) 2 (1 Mbit/sec) 4 (2 Mbit/sec) (default) 11 (5.5 Mbit/sec) 22 (11 Mbit/sec)	RW	txrate
Supported Frequency Channels	Octet String	Depends on Regulatory Domain	R	suppchannels
Physical Layer Type	Integer	ds (direct sequence spread spectrum) for 802.11b	R	phytype
Regulatory Domain List	DisplayString	USA (FCC) Canada (DOC) Europe (ETSI) Spain (SP) France (FR) Japan (MKK)	R	regdomain



NOTE

There is an inter-dependent relationship between the Distance between APs and the Multicast Rate. In general, larger systems operate a lower average transmit rates.

Distance between APs	Multicast Rate
Large	1 and 2 Mbits/sec
Medium	1, 2, and 5.5 Mbits/sec
Small	1, 2, 5.5 and 11 Mbits/sec
Minicell	1, 2, 5.5 and 11 Mbits/sec
Microcell	1, 2, 5.5 and 11 Mbits/sec

Wireless Distribution System (WDS) Parameters



NOTE

These parameters only apply to 802.11b radios.

Name	Type	Values	Access	CLI Parameter
WDS Table	Table	N/A	R	wdstbl
Port Index	Integer	3.1 - 3.6 (Wireless A) 4.1 - 4.6 (Wireless B)	R	portindex
Status	Integer	enable (1) disable (2) (default)	RW	status
Partner MAC Address	PhysAddress	User Defined	RW	partnermacaddr

Using the Command Line Interface

Wireless 802.11a Parameters

Name	Type	Values	Access	CLI Parameter
Wireless Interfaces	Group	N/A	R	wif
Network Name	DisplayString	2 – 31 characters My Wireless Network A (default) My Wireless Network B (default)	RW	netname
Auto Channel Select (ACS)	Integer	enable (default) disable	RW	autochannel
DTIM Period	Integer	1 – 65535 (1 = default)	RW	dtimperiod
Operating Frequency Channel	Integer	36 - 5.180 GHz 40 - 5.200 GHz 44 - 5.220 GHz 48 - 5.240 GHz 52 - 5.260 GHz (default FCC) 56 - 5.280 GHz 60 - 5.300 GHz 64 - 5.320 GHz Channels 36-64 are valid for the FCC and ETSI regulatory domains. The following channels are available in Japan: 34 - 5.170 GHz (default) 38 - 5.190 GHz 42 - 5.210 GHz 46 - 5.230 GHz	RW	channel
RTS/CTS Medium Reservation	Integer	0 – 2347 Default is 2347 (off)	RW	medres
MAC Address	PhyAddress	12 hex digits	R	macaddr
Supported Data Rates	Octet String	See "Transmit Rate"	R	suppdatarates
Transmit Rate	Integer32	Reported in 500 Kb/sec intervals: 0 - Auto Fallback (default) 12 (6 Mbit/sec) 18 (9 Mbits/sec) 24 (12 Mbits/sec) 36 (18 Mbits/sec) 48 (24 Mbits/sec) 72 (36 Mbits/sec) 96 (48 Mbits/sec) 108 (54 Mbits/sec)	RW	txrate
Supported Frequency Channels	Octet String	See Operating Frequency Channel	R	suppchannels
Physical Layer Type	Integer	ofdm (orthogonal frequency division multiplexing) for 802.11a	R	phytype
Regulatory Domain List	DisplayString	USA (FCC) Canada (DOC) Europe (ETSI) Spain (SP) France (FR) Japan (MKK)	R	regdomain



NOTE

For 802.11a cards in Europe, Auto Channel Select is a read-only parameter; it is always enabled.

Using the Command Line Interface

Ethernet Interface Parameters

Name	Type	Values	Access	CLI Parameter
Ethernet Interface	Group	N/A	R	ethernet
Speed	Integer	10halfduplex 10fullduplex 10autoduplex 100halfduplex 100fullduplex autohalfduplex autoautoduplex (default)	RW	etherspeed
MAC Address	PhyAddress	N/A	R	ethermacaddr

Management Parameters

IP Access Table Parameters

When creating table entries, you may either specify the argument name followed by argument value or simply entering the argument value. When only the argument value is specified, then enter the values in the order depicted by the following table. CLI applies default values to the omitted arguments. Due to the nature of the information, the only argument that can be omitted is the “comment” argument.

Name	Type	Values	Access	CLI Parameter
IP Access Table	Table	N/A	R	mgmtipaccesstbl
Table Index	Integer	User Defined	N/A	index
IP Address	IpAddress	User Defined	RW	ipaddr
IP Mask	IpAddress	User Defined	RW	ipmask
Comment (optional)	DisplayString	User Defined	RW	cmt
Status (optional)	Integer	enable disable delete	RW	status

Access Control Parameters

Name	Type	Values	Access	CLI Parameter
Access Control	Group	N/A	R	accessctl
Access Control On	Integer	disable (0) enable (1)	RW	accessControlOn
Access Control Table	Table	N/A	RW	acIpRangeTable
Access Control Table Index	Integer	N/A	R	acIpRangeIndex
Access Control Range Starting IP Address	IpAddress	User Defined	RW	acIpRangeStartAddress
Access Control Range Starting IP Address	IpAddress	User Defined	RW	acIpRangeEndAddress
Access Control IP Table Entry Status	RowStatus	active (1), notInService (2), notReady (3), createAndGo (4), createAndWait (5), destroy (6)	RW	acIpRangeEntryStatus



NOTE

Both the IP Access Table Parameters and the Access Control Parameters determine which IP addresses are allowed to manage the AP over the Ethernet interface.

Using the Command Line Interface

SNMP Parameters

Name	Type	Values	Access	CLI Parameter
SNMP	Group	N/A	R	snmp
SNMP Management Interface Bitmask	Interface Bitmask	0 - no interfaces (disable) 1 - Ethernet 4 - Wireless A 8- Wireless B 15 - all interfaces	RW	snmpifbitmask
Read Password	DisplayString	User Defined public (default) max 63 characters	W	snmprpasswd
Read/Write Password	DisplayString	User Defined public (default) max 63 characters	W	snmprwpasswd
SNMP Trap Host Table	N/A	N/A	R	snmptraphosttbl

SNMP Table Host Table Parameters

When creating table entries, you may either specifying the argument name followed by argument value. CLI applies default values to the omitted arguments. Due to the nature of the information, the only argument that can be omitted is the "comment" argument.

Name	Type	Values	Access	CLI Parameter
SNMP Trap Host Table	Table	N/A	R	snmptraphosttbl
Table Index	Integer	User Defined	N/A	index
IP Address	IpAddress	User Defined	RW	ipaddr
Password	DisplayString	User Defined	W	passwd
Comment (optional)	DisplayString	User Defined	RW	cmt
Status (optional)	Integer	enable disable delete	RW	status

Telnet Parameters

Name	Type	Values	Access	CLI Parameter
Telnet	Group	N/A	R	telnet
Telnet Management Interface Bitmask	Interface Bitmask	0 - no interfaces (disable) 1 - Ethernet 4 - Wireless A 8- Wireless B 15 - all interfaces	RW	telifbitmask
Telnet Port	Integer	User Defined 23 (default)	RW	telport
Telnet Login Inactivity Time-out	Integer	1 - 60 seconds 30 sec (default)	RW	tellovertimeout
Telnet Session Idle Time-out	Integer	1 - 900 seconds 900 sec (default)	RW	telsessiontimeout

Using the Command Line Interface

Serial Port Parameters

Name	Type	Values	Access	CLI Parameter
Serial	Group	N/A	R	serial
Baud Rate	Integer	2400, 4800, 9600 (default), 19200, 38400, 57600	RW	serbaudrate
Data Bits	Integer	8	R	serdatabits
Parity	Integer	none	R	serparity
Stop Bits	Integer	1	R	serstopbits
Flow Control	Value	none (default) xon/xoff	RW	serflowctrl

HTTP (web browser) Parameters

Name	Type	Values	Access	CLI Parameter
HTTP	Group	N/A	R	http
HTTP Management Interface Bitmask	Interface Bitmask	0 - no interfaces (disable) 1 - Ethernet 4 - Wireless A 8 - Wireless B 15 - all interfaces	RW	httpifbitmask
HTTP Password	DisplayString	User Defined max 64 characters	W	httppasswd
HTTP Port	Integer	User Defined Default = 80	RW	httpport
Help Link	DisplayString	User Defined	RW	httphelplink

TFTP Server Parameters

These parameters relate to upload and download commands.

When a user executes an upload and/or download Command, the specified arguments are stored in TFTP parameters for future use. If nothing is specified in the command line when issuing subsequent upload and/or download commands, the stored arguments are used.

Name	Type	Values	Access	CLI Parameter
TFTP	Group	N/A	R	tftp
TFTP Server IP Address	IpAddress	User Defined	RW	tftpipaddr
TFTP File Name	DisplayString	User Defined	RW	tftpfilename
TFTP File Type	Integer	img config bootloader generic	RW	tftpfiletype

Using the Command Line Interface

NTP Parameters

Name	Type	Values	Access	CLI Parameter
SNTP	Group	N/A	R	sntp
SNTP On	Integer	enable (1) disable (2)	RW	oriSNTPStatus
Primary SNTP Server IP	DisplayString	User Defined	RW	oriSNTPPrimaryServerNameOrIPAddress
Secondary SNTP Server IP	DisplayString	User Defined	RW	oriSNTPSecondaryServerNameOrIPAddress
Time Zone Setup	Integer	dateline (1) samoa (2) hawaii (3) alaska (4) pacific-us (5) mountain-us (6) arizona (7) central-us (8) mexico-city (9) eastern-us (10) indiana (11) atlantic-canada (12) santiago (13) newfoundland (14) brasil (15) buenos-aires (16) mid-atlantic (17) azores (18) london (19) western-europe (20) eastern-europe (21) cairo (22) russia-iraq (23) iran (24) arabian (25) afghanistan (26) pakistan (27) india (28) bangladesh (29) burma (30) bangkok (31) australia-wt (32) hong-kong (33) beijing (34) japan-korea (35) australia-ct (36) australia-et (37) central-pacific (38) new-zealand (39) tonga (40) western-samoa (41)	RW	oriSNTPTimeZone
Date and Time	DisplayString	N/A	R	oriSNTPDateAndTime
Daylight Saving Adjustment	Integer	plus-two (1) plus-one (2) unchanged (3) minus-one (4) minus-two (5)	RW	oriSNTPDayLightSavingTime
Year	Integer32	User Defined	RW	oriSNTPYear
Month	Integer32 (1..12)	User Defined	RW	oriSNTPMonth

Using the Command Line Interface

Day	Integer32 (1..31)	User Defined	RW	oriSNTPDay
Hour	Integer32 (0..23)	User Defined	RW	oriSNTPHour
Minutes	Integer32 (0..59)	User Defined	RW	oriSNTPMinutes
Seconds	Integer32 (0..59)	User Defined	RW	oriSNTPSeconds

Security Parameters



NOTE

The Security group is not currently implemented in the AP-2500.

Name	Type	Values	Access	CLI Parameter
Security	Group	N/A	R	security
Configuration Mode	Integer	not currently implemented	R	secconfig

RADIUS Server Parameters

Name	Type	Values	Access	CLI Parameter
AAA RADIUS	Group	N/A	R	aaaRadius
AAA RADIUS Authentication On	Integer	disable (0) enable (1)	RW	aaaRadiusAuthOn
Primary RADIUS Authentication Server IP	IpAddress	User Defined	RW	aaaRadiusAuthSrv1Ip
Primary RADIUS Auth Server Port	Integer	User Defined	RW	aaaRadiusAuthSrv1Port
Primary RADIUS Auth Server Secret Key	DisplayString Size(0..130)	User Defined	RW	aaaRadiusAuthSrv1Sec
Primary RADIUS Auth Server DNS Name	DisplayString Size(0..240)	User Defined	RW	aaaRadiusAuthSrv1Dns
Secondary RADIUS Authentication Server IP	IpAddress	User Defined	RW	aaaRadiusAuthSrv2Ip
Secondary RADIUS Auth Server Port	Integer	User Defined	RW	aaaRadiusAuthSrv2Port
Secondary RADIUS Auth Server Secret Key	DisplayString Size(0..130)	User Defined	RW	aaaRadiusAuthSrv2Sec
Secondary RADIUS Auth Server DNS Name	DisplayString Size(0..240)	User Defined	RW	aaaRadiusAuthSrv2Dns
AAA RADIUS Accounting	Group	N/A	R	aaaRadiusAcct
AAA RADIUS Accounting On	Integer	disable (0) enable (1)	RW	aaaRadiusAcctOn
Primary RADIUS Accounting Server IP	IpAddress	User Defined	RW	aaaRadiusAcctSrv1Ip
Primary RADIUS Acct Server Port	Integer	User Defined	RW	aaaRadiusAcctSrv1Port

Using the Command Line Interface

Primary RADIUS Acct Server Secret Key	DisplayString Size(0..130)	User Defined	RW	aaaRadiusAcctSrv1Sec
Primary RADIUS Acct Server DNS Name	DisplayString Size(0..240)	User Defined	RW	aaaRadiusAcctSrv1Dns
Secondary RADIUS Accounting Server IP	IpAddress	User Defined	RW	aaaRadiusAcctSrv2Ip
Secondary RADIUS Acct Server Port	Integer	User Defined	RW	aaaRadiusAcctSrv2Port
Secondary RADIUS Acct Server Secret Key	DisplayString Size(0..130)	User Defined	RW	aaaRadiusAcctSrv2Sec
Secondary RADIUS Acct Server DNS Name	DisplayString Size(0..240)	User Defined	RW	aaaRadiusAcctSrv2Dns
AAA RADIUS ISP Account Creation	Integer	disable (0) enable (1)	RW	aaaRadiusIspRedirectOn
AAA RADIUS ISP Server URL	DisplayString Size(0..238)	User Defined	RW	aaaRadiusIspUrl
AAA RADIUS ISP Account Server URL	DisplayString Size(0..238)	User Defined	RW	aaaRadiusIspCreateUrl
AAA RADIUS ISP Server IP	IpAddress	User Defined	RW	aaaRadiusIspServerIp
AAA RADIUS Profile Caching	Integer	disable (0) enable (1)	RW	aaaRadiusCacheOn
AAA RADIUS Retransmission Method	Integer	failover (0) round-robin (1)	RW	aaaRadiusRetransMethod
AAA RADIUS Retransmission Frequency	Integer	User Defined	RW	aaaRadiusRetransFreq
AAA RADIUS Retransmission Attempts	Integer	User Defined	RW	aaaRadiusRetransAttempts
AAA RADIUS Retransmission Timeout	Integer	User Defined	RW	aaaRadiusRetransTimeout
AAA RADIUS Subscriber Timeout	Integer	User Defined	RW	aaaRadiusDefaultIdle
Radius Username Type	Integer	user-input (0) mac-mac (1) mac-key (2)	RW	aaaRadiusUsernameType
AAA RADIUS NAS ID Enable	Integer	disable (0) enable (1)	RW	aaaRadiusNasIdOn
AAA RADIUS NAS ID	DisplayString Size(0..32)	User Defined	RW	aaaRadiusNasId
AAA RADIUS NAS IP Enable	Integer	disable (0) enable (1)	RW	aaaRadiusNasIpOn
AAA RADIUS NAS Port Enable	Integer	disable (0) enable (1)	RW	aaaRadiusNasPortOn
AAA RADIUS NAS Port Type	Integer	User Defined	RW	aaaRadiusNasPortType
AAA RADIUS Frame IP Enable	Integer	disable (0) enable (1)	RW	aaaRadiusFipOn
AAA RADIUS URL Redirection	Integer	disable (0) enable (1)	RW	aaaRadiusRedUrlOn

Using the Command Line Interface

Encryption Parameters

The following table details the WEP encryption parameters for the AP-2500. This information applies to both the 802.11a and the 802.11b wireless interfaces.

Name	Type	Values	Access	CLI Parameter
Wireless Interfaces Security	Group		R	wifsec
Encryption Status	Integer	enable disable	RW	encryptstatus
Index	Integer	3 = PC Card A 4 = PC Card B	N/A	N/A
Encryption Key 1	DisplayString	User Defined	W	encryptkey1
Encryption Key 2	DisplayString	User Defined	W	encryptkey2
Encryption Key 3	DisplayString	User Defined	W	encryptkey3
Encryption Key 4	DisplayString	User Defined	W	encryptkey4
Deny non-encrypted Data	Integer	enable (default) disable	RW	encryptdeny
Data Transmission Encryption Key	Integer	1 (default) 2 3 4	RW	encryptkeytx

Security Encryption Key Length Table

The following table details how to set the Encryption Key Length for the wireless interfaces.

Name	Type	Values	Access	CLI Parameter
Security Encryption Key Length Table	Table	N/A	R	secenckeylentbl
Index	Integer	3 = PC Card A 4 = PC Card B	N/A	index
Encryption Key Length	Integer	64 bit 128 bit	RW	enckeylen



NOTE

The available Encryption Key Lengths vary based on card type. Depending on the model, 802.11b cards support 64 (also referred to as 40) bits or 128 (also referred to as 104) bits. 802.11a cards support 64 (also referred to as 40) or 128 (also referred to as 104) bits.

VPN

See [Miscellaneous Parameters](#) for VPN commands.

Home Page Redirection Parameters

Name	Type	Values	Access	CLI Parameter
Home Page Redirection	Group	N/A	R	hpr
Home Page Redirection Enabled	Integer	disable (0) enable (1)	RW	hprOn
HPR URL	DisplayString Size(0..238)	User Defined	RW	hprUrl
HPR Parameters Passing	Integer	disable (0) enable (1)	RW	hprParameterPassing
HPR Frequency (mins.)	Integer	User Defined	RW	hprRedirectionFrequency

Using the Command Line Interface

AAA Parameters

The Authentication, Authorization and Accounting (AAA) module enables solution provider to provision, track, and bill new or returning subscribers. These parameters are shown in the following tables.

Basic AAA Parameters

Name	Type	Values	Access	CLI Parameter
AAA Group	Group	N/A	R	AAA
AAA Service	Integer	disable (0) enable (1)	RW	aaaOn
AAA XML Service	Integer	disable (0) enable (1)	RW	aaaXmlOn
AAA XML Server IP	IpAddress	User Defined	RW	aaaXmlSenderIdp
AAA Passthrough Port	Integer	disable (0) enable (1)	RW	aaaPassthroughPortOn
AAA Passthrough Port Number	Integer	User Defined	RW	aaaPassthroughPortNumber
Authorization Mode	Integer	internalAuthorization(0) externalAuthorization(1)	RW	aaaAuthMode

AAA External Authorization Parameters

Name	Type	Values	Access	CLI Parameter
AAA External Authorization	Group	N/A	R	aaaExternalAuth
Secret Key	DisplayString Size(0..32)	User Defined	RW/Reboot	aaaSecretKey
External Authorization Server IP	IpAddress	User Defined	RW	aaaExternalIpAddress
External Authorization Server URL	DisplayString Size(0..238)	User Defined	RW	aaaAuthorizationUrl

Using the Command Line Interface

AAA Internal Authorization Parameters

Name	Type	Values	Access	CLI Parameter
AAA Internal Authorization	Group	N/A	R	aaaInternalAuth
SSL Support	Integer	disable (0) enable (1)	RW/Reboot	aaaSslOn
SSL Host Name	DisplayString Size(0..31)	User Defined	RW	aaaSslHostName
SSL Portal Page Redirection	Integer	disable (0) enable (1)	RW	aaaPortalPageOn
SSL Portal Page URL	DisplayString Size(0..238)	User defined	RW	aaaPortalPageUrl
Enable User Name and Password	Integer	disable (0) enable (1)	RW	aaaUsernameOn
Allow New Subscriber	Integer	disable (0) enable (1)	RW	aaaNewSubscriberOn
Credit Card Service	Integer	disable (0) enable (1)	RW	aaaCreditCardOn
Credit Card Service Server URL	DisplayString Size(0..238)	User defined	RW	aaaCreditCardUrl
Credit Card Service Server IP	IpAddress	User Defined	RW	aaaCreditCardIp
Merchant ID for Credit Card Service	DisplayString Size(0..32)	User Defined	RW	aaaMerchantId
Smart Client Support	Integer	disable (0) enable (1)	RW	aaaSmartClientOn

Logging Parameters

Name	Type	Values	Access	CLI Parameter
NSE Log System	Group	N/A	R	log
System Logging On	Integer	disable (0) enable (1)	RW	systemLoggingOn
System Log Number	Integer	0..7	RW	systemLogNumber
Syslog Server IP	IpAddress	User Defined	RW	systemLogServerIp
AAA Logging	Integer	disable (0) enable (1)	RW	aaaLoggingOn
AAA Log Number	integer	0 – 7	RW	aaaLogNumber
AAA SYSLOG Server IP	IpAddress	User Defined	RW	aaaLogServerIp

Using the Command Line Interface

URL Filtering Parameters

Name	Type	Values	Access	CLI Parameter
URL Filtering	Group	N/A	R	urlFiltering
URL Filtering On	Integer	disable (0) enable (1)	RW	urlFilteringOn

URL Filtering IP Table

Name	Type	Values	Access	CLI Parameter
URL Filtering IP Table	Table	N/A	R	urlFilteringIPTable
URL Filtering IP Table Index	Integer	N/A	R	urlFilteringIPTableIndex
URL Filtering IP Table Address	DisplayString Size(1..15)	User Defined	RW	urlFilteringIPTableAddress
URL Filtering IP Table Status	RowStatus	active (1), notInService (2), notReady (3), createAndGo (4), createAndWait (5), destroy (6)	RW	urlFilteringIPTableStatus

URL Filtering DNS Table

Name	Type	Values	Access	CLI Parameter
URL Filtering DNS Table	Table	N/A	R	urlFilteringDNSTable
URL Filtering DNS Table Index	Integer	N/A	R	urlFilteringDNSTableIndex
URL Filtering DNS Table Name	DisplayString Size(0..237)	User Defined	RW	urlFilteringDNSTableAddress
URL Filtering DNS Table Status	RowStatus	active (1), notInService (2), notReady (3), createAndGo (4), createAndWait (5), destroy (6)	RW	urlFilteringDNSTableStatus

Using the Command Line Interface

ICC (Information Control Console) Parameters

Name	Type	Values	Access	CLI Parameter
ICC	Group	N/A	R	icc
ICC On	Integer	disable (0) enable (1)	RW	iccOn
Title to display on ICC Console	DisplayString Size(0..238)	User Defined	RW	iccTitle
ICC Logout Option	Integer	redisplay (0) logout (2)	RW	iccLogoutOption
ICC Language Option	Integer	english (0)	RW	iccLanguageOption
ICC Character Set Option	Integer	default (0) western-iso-8859-1 (1) chinese-big5 (2) chinese-euc-cn (3) chinese-euc-tw (4) chinese-gb2312 (5) japanese-euc-jp (6) japanese-iso-2022-jp (7) japanese-shift-jis (8) korean-euc-kr (9) korean-iso-2022-kr (10) korean-ks-c-5601 (11)	RW	iccCharSetOption
ISP Logo Button Name	DisplayString Size(0..37)	User Defined	RW	icclSPLogoButtonName
ISP Logo Button URL	DisplayString Size(0..238)	User Defined	RW	icclSPLogoButtonURL
ISP Logo Button Image Name	DisplayString Size(0..31)	User Defined	RW	icclSPLogoButtonImgName

ICC Button Configuration

The following table is for ICC Button 2. The same parameters apply to button 3 through 9 (simply change the 2 in each command to a different button number).

Name	Type	Values	Access	CLI Parameter
ICC Button Name 2	DisplayString Size(0..37)	User Defined	RW	iccButtonName2
ICC Button URL 2	DisplayString Size(0..238)	User Defined	RW	iccButtonURL2
ICC Button Image Name 2	DisplayString Size(0..31)	User Defined	RW	iccButtonImgName2

Using the Command Line Interface

ICC Banner Configuration

The following table is for ICC Banner 1. The same parameters apply to banners 2 through 5 (simply change the 1 in each command to a different button number).

Name	Type	Values	Access	CLI Parameter
ICC Banner 1 Name	DisplayString Size(0..16)	User Defined	RW	iccBannerName1
ICC Banner 1 URL	DisplayString Size(0..238)	User Defined	RW	iccBannerURL1
ICC Banner 1 Image Name	DisplayString Size(0..31)	User Defined	RW	iccBannerImgName1
ICC Banner 1 Duration	Integer	User Defined	RW	iccBannerDuration1
ICC Banner 1 Start Time	DisplayString Size(1..16)	User Defined	RW	iccBannerStartTime1
ICC Banner 1 Stop Time	DisplayString Size(0..16)	User Defined	RW	iccBannerStopTime1

SMTP Parameters

Name	Type	Values	Access	CLI Parameter
SMTP Service	Group	N/A	R	smtp
SMTP Redirection	Integer	disable (0) enable (1)	RW	smtpRedirect
SMTP Server IP	IpAddress	User Defined	RW	smtpServerIP
SMTP Properly Configureds Redirection	Integer	disable (0) enable (1)	RW	smtpPcRedirect

Passthrough Parameters

“Passthrough” allows non subscriber to access predetermined services at the solution provider’s discretion. This is useful if providers wanted to openly promote selected services to all users.

Name	Type	Values	Access	CLI Parameter
Passthrough Feature	Group	N/A	R	passthru
Passthrough Service On	Integer	disable (0) enable (1)	RW	passthroughOn

Using the Command Line Interface

Passthru IP Table

Name	Type	Values	Access	CLI Parameter
Passthru IP Table	Table	N/A	R	passthroughIPTable
Passthru IP Table Index	Integer	N/A	R	passthroughIPTableIndex
Passthru IP Table Address	IpAddress	User Defined	RW	passthroughIPTableAddress
Passthru IP Table Status	RowStatus	active (1), notInService (2), notReady (3), createAndGo (4), createAndWait (5), destroy (6)	RW	passthroughIPTableStatus

Passthru DNS Table

Name	Type	Values	Access	CLI Parameter
Passthru DNS Table	Table	N/A	R	passthroughDNSTable
Passthru DNS Table Index	Integer	N/A	R	passthroughDNSTableIndex
Passthru DNS Table Name	DisplayString Size(0..238)	User Defined	RW	passthroughDNSTableName
Passthru DNS Table Status	RowStatus	active (1), notInService (2), notReady (3), createAndGo (4), createAndWait (5), destroy (6)	RW	passthroughDNSTableStatus

AAA Passthrough Port

See [Basic AAA Parameters](#).

Bandwidth Management Parameters

System administrators can manage the bandwidth for subscribers, defined in Kbps (Kilobits per second) for both upstream and downstream data transmissions.

Name	Type	Values	Access	CLI Parameter
Bandwidth Management	Group	N/A	R	bwmgmt
Bandwidth Management Service	Integer	disable (0) enable (1)	RW/Reboot	bandwidthManagementOn
WAN Uplink Bandwidth	Integer	User Defined	RW/Reboot	bwmUpWanLinkSpeed
WAN Downlink Bandwidth	Integer	User Defined	RW/Reboot	bwmDownWanLinkSpeed

Using the Command Line Interface

Billing Parameters

Name	Type	Values	Access	CLI Parameter
AAA Billing Option	Group	N/A	R	aaaBillingOption
Intro Message	DisplayString Size(0..140)	User Defined	RW	aaaBilloptIntroMsg
Offer Message	DisplayString Size(0..140)	User Defined	RW	aaaBilloptOfferMsg
Policy Message	DisplayString Size(0..117)	User Defined	RW	aaaBilloptPolicyMsg
Billing Rate Time Unit	Integer	minute (0), hour (1), day (2), week (3), month (4)	RW	aaaBilloptRateShow
Minimum Time Unit	Integer	User Defined	RW	aaaBilloptMinTimeUnit
Free Access Time	Integer	User Defined	RW	aaaBilloptFreeAccessTime
Max Free Access Time	Integer	User Defined	RW	aaaBilloptMaxSubLifetime

Billing Mirroring Parameters

Name	Type	Values	Access	CLI Parameter
Billing Record Mirror	Group	N/A	R	billRecMirror
Bill Record Mirror On	Integer	disable (0) enable (1)	RW	brmMirrorOn
Property ID	DisplayString Size(1..32)	User Defined	RW	brmPropertyId
AP ID	DisplayString Size(1..32)	N/A	R	brmUsgid
Primary Mirroring Server IP	IpAddress	User Defined	RW	brmServerIpPrimary
Primary Mirroring Server URL	DisplayString Size(1..238)	User Defined	RW	brmServerUrlPrimary
Primary Mirroring Server Secret Key	DisplayString Size(0..32)	User Defined	RW	brmServerSecretPrimary
Primary Mirroring Server Port	Integer	User Defined	RW	brmServerPortPrimary
Secondary Mirroring Server IP	IpAddress	User Defined	RW	brmServerIpSecondary
Secondary Mirroring Server URL	DisplayString Size(1..238)	User Defined	RW	brmServerUrlSecondary
Secondary Mirroring Server Secret Key	DisplayString Size(0..32)	User Defined	RW	brmServerSecretSecondary
Secondary Mirroring Server Port	Integer	User Defined	RW	brmServerPortSecondary
Carbon Copy Server IP One	IpAddress	User Defined	RW	brmServerCCIpOne

Using the Command Line Interface

Carbon Copy Server URL One	DisplayString Size(1..238)	User Defined	RW	brmServerCCUrlOne
Carbon Copy Server Secret Key One	DisplayString Size(0..32)	User Defined	RW	brmServerCCSecretOne
Carbon Copy Server Port One	Integer	User Defined	RW	brmServerCCPortOne
Carbon Copy Server IP Two	IpAddress	User Defined	RW	brmServerCCIpTwo
Carbon Copy Server URL Two	DisplayString Size(1..238)	User Defined	RW	brmServerCCUrlTwo
Carbon Copy Server Secret Key Two	DisplayString Size(0..32)	User Defined	RW	brmServerCCSecretTwo
Carbon Copy Server Port Two	Integer	User Defined	RW	brmServerCCPortTwo
Carbon Copy Server IP Three	IpAddress	User Defined	RW	brmServerCCIpThree
Carbon Copy Server URL Three	DisplayString Size(1..238)	User Defined	RW	brmServerCCUrlThree
Carbon Copy Server Secret Key Three	DisplayString Size(0..32)	User Defined	RW	brmServerCCSecretThree
Carbon Copy Server Port Three	Integer	User Defined	RW	brmServerCCPortThree
Retransmit Method	Integer	alternate (1) notAlternate (2)	RW	brmRetransMethod
Retransmit Attempts	Integer	User Defined	RW	brmRetransAttempts
Retransmit Delay	Integer	User Defined	RW	brmRetransDelay

Billing Plans Configuration

The following table is for Billing Plan 0. The same parameters apply to Billing Plans 1 through 5 (simply change the **0** in each command to a different billing plan number).

Name	Type	Values	Access	CLI Parameter
AAA Billing Plan 0	Group	N/A	R	aaaBillingPlan0
Billing Plan Enabled	Integer	disable (0) enable (1)	RW	aaaBillingPlanOn0
Plan Label	DisplayString Size(0..16)	User Defined	RW	aaaBillingPlanLabel0
Plan Description	DisplayString Size(0..140)	User Defined	RW	aaaBillingPlanDesc0
Rate per Minute	DisplayString Size(0..32)	User Defined	RW	aaaBillingPlanMin0
Rate per Hour	DisplayString Size(0..32)	User Defined	RW	aaaBillingPlanHour0
Rate per Day	DisplayString Size(0..32)	User Defined	RW	aaaBillingPlanDay0
Rate per Week	DisplayString Size(0..32)	User Defined	RW	aaaBillingPlanWeek0

Using the Command Line Interface

Rate per Month	DisplayString Size(0..32)	User Defined	RW	aaaBillingPlanMonth0
Uplink Bandwidth	Integer	0..1500	RW	aaaBillingPlanBandwidthUp0
Downlink Bandwidth	Integer	0..1500	RW	aaaBillingPlanBandwidthDown0
DHCP Pool	Integer	private (0) public (1)	RW	aaaBillingPlanDHCPPool0

Subscriber Messages Parameters

Name	Type	Values	Access	CLI Parameter
AAA Subscriber Login UI	Group	N/A	R	aaaSubLoginUI
Service Selection Message	DisplayString Size(0..140)	User Defined	RW	aaaWebServiceMsg
Existing User Message	DisplayString Size(0..140)	User Defined	RW	aaaWebExistingUserMsg
New User Message	DisplayString Size(0..140)	User Defined	RW	aaaWebNewUsernameMsg
Contact Message	DisplayString Size(0..140)	User Defined	RW	aaaWebContactMsg
Java Script Enabled	Integer	disable (0) enable (1)	RW	aaaWebJavascriptOn
Remember Me Cookie Enaled	Integer	disable (0) enable (1)	RW	aaaWebRememberMeOn
Remember Me Message	DisplayString Size(0..140)	User Defined	RW	aaaRememberMeMsg
Days to Retain Remember Me Cookie	Integer	User Defined	RW	aaaRememberMeDays
Currency Symbol	DisplayString Size(0..16)	User Defined	RW	aaaCurrency
Decimals in Currency	Integer	User Defined	RW	aaaAmountDecimals
Image Filename	DisplayString Size(0..140)	User Defined	RW	aaaWebImage
Background Color	DisplayString Size(0..140)	User Defined	RW	aaaWebPageBgcolor
Table Background Color	DisplayString Size(0..140)	User Defined	RW	aaaWebTabBgcolor
Title Font	DisplayString Size(0..140)	User Defined	RW	aaaWebTitleFont
Line item Font	DisplayString Size(0..140)	User Defined	RW	aaaWebItemFont
Password Required	DisplayString Size(0..218)	User Defined	RW	aaaErrorAccessPassword
An Error Occurred	DisplayString Size(0..218)	User Defined	RW	aaaErrorHasOccurred

Using the Command Line Interface

ISP Challenge	DisplayString Size(0..218)	User Defined	RW	aaaErrorISPChallenge
Value Out of Range	DisplayString Size(0..218)	User Defined	RW	aaaErrorMinMaxValues
No Billing Options	DisplayString Size(0..218)	User Defined	RW	aaaErrorNoBillingOpts
Internet Service Not Available	DisplayString Size(0..218)	User Defined	RW	aaaErrorNotAvailable
Password Unmatched	DisplayString Size(0..218)	User Defined	RW	aaaErrorPasswordMatch
Wrong Password	DisplayString Size(0..218)	User Defined	RW	aaaErrorPasswordWrong
Too Many Subscribers	DisplayString Size(0..218)	User Defined	RW	aaaErrorTooManyUsers
Try Again	DisplayString Size(0..218)	User Defined	RW	aaaErrorTryAgain
User ID Not Found	DisplayString Size(0..218)	User Defined	RW	aaaErrorUserIdMissing
User ID Taken	DisplayString Size(0..218)	User Defined	RW	aaaErrorUserIdTaken
We Are Sorry	DisplayString Size(0..218)	User Defined	RW	aaaErrorWeAreSorry
Whole Number Only	DisplayString Size(0..218)	User Defined	RW	aaaErrorWholeNumber
Check Username and Password	DisplayString Size(0..218)	User Defined	RW	aaaErrorYourAccount
Billing Mode Message	DisplayString Size(0..218)	User Defined	RW	aaaMessageBillingMode
Bill by Credit Card Message	DisplayString Size(0..218)	User Defined	RW	aaaMessagebyCreditCard
Choose User ID Message	DisplayString Size(0..218)	User Defined	RW	aaaMessageChooseUsername
Choose Password Message 1	DisplayString Size(0..218)	User Defined	RW	aaaMessageChoosePasswd1
Choose Password Message 2	DisplayString Size(0..218)	User Defined	RW	aaaMessageChoosePasswd2
Free Internet Message	DisplayString Size(0..218)	User Defined	RW	aaaMessageFreeInternet
New User Login Message	DisplayString Size(0..218)	User Defined	RW	aaaMessageNewUserLogin
Existing User Login Message	DisplayString Size(0..218)	User Defined	RW	aaaMessageOldUserLogin
Purchase OK Message 1	DisplayString Size(0..218)	User Defined	RW	aaaMessagePurchaseOK1
Purchase OK Message 2	DisplayString Size(0..218)	User Defined	RW	aaaMessagePurchaseOK2
Purchase Select Message	DisplayString Size(0..218)	User Defined	RW	aaaMessagePurchaseSelect
Purchase Time Message	DisplayString Size(0..218)	User Defined	RW	aaaMessagePurchaseTime

Using the Command Line Interface

RADIUS Create Message	DisplayString Size(0..218)	User Defined	RW	aaaMessageRadiusCreate
RADIUS Login Message	DisplayString Size(0..218)	User Defined	RW	aaaMessageRadiusLogin
Request Failed Message	DisplayString Size(0..218)	User Defined	RW	aaaMessageRequestFailed
Request Granted Message	DisplayString Size(0..218)	User Defined	RW	aaaMessageRequestGranted
Thank You Message	DisplayString Size(0..218)	User Defined	RW	aaaMessageThankYou
Verifying Message	DisplayString Size(0..218)	User Defined	RW	aaaMessageVerifying
Purchase Options Message	DisplayString Size(0..218)	User Defined	RW	aaaMessageYourPurchase

Authorized Subscribers Table

Name	Type	Values	Access	CLI Parameter
AAA Authorized Subscriber Table	Table	N/A	R	aaaSubCurrTable
Subscriber Index	Integer	N/A	R	authSubIndex
Subscriber Type	Integer	subscriber (0), device (1)	RW	authSubType
DHCP Address Type	Integer	private (0), public (1)	RW	authSubDhcpAddrType
Device Port	Integer	User Defined	RW	authSubDevicePort
Subscriber MAC	DisplayString Size(0..17)	User Defined	RW	authSubMac
Subscriber IP	IpAddress	User Defined	RW	authSubIp
Subscriber Name	DisplayString Size(0..96)	User Defined	RW	authSubName
Subscriber Password	DisplayString Size(0..32)	User Defined	RW	authSubPassword
Subscriber Expiration Time (Hrs)	Integer	User Defined	RW	authSubExpTimeHrs
Subscriber Expiration Time (Mins)	Integer	0..59	RW	authSubExpTimeMins
Subscriber Amount Paid	DisplayString Size(0..17)	User Defined	RW	authSubAmtPaid
Subscriber Amount Left	DisplayString	N/A	R	authSubAmtLeft
Optional Notation 1	DisplayString Size(0..16)	User Defined	RW	authSubUser1
Optional Notation 2	DisplayString Size(0..16)	User Defined	RW	authSubUser2
Subscriber Upload Bandwidth	Integer	User Defined	RW	authSubBwUp

Using the Command Line Interface

Subscriber Download Bandwidth	Integer	User Defined	RW	authSubBwDown
Credit Card Confirmation Number	DisplayString	N/A	R	authSubConfirmation
Subscriber Status	RowStatus	active (1), notInService (2), notReady (3), createAndGo (4), createAndWait (5), destroy (6)	RW	authSubStatus

Current Subscribers Table

Name	Type	Values	Access	CLI Parameter
AAA Current Subscriber Table	Table	N/A	R	aaaSubCurrTable
Subscriber Index	Integer	N/A	R	subIndex
Subscriber MAC	DisplayString	N/A	R	subMac
Subscriber IP	IpAddress	N/A	R	subIp
Subscriber Port	Integer	N/A	R	subPort
Subscriber Name	DisplayString	N/A	R	subName
Subscriber Upload Bandwidth	Integer	N/A	R	subBwUp
Subscriber Download Bandwidth	Integer	N/A	R	subBwDown
Subscriber AAA State	DisplayString	N/A	R	subAaaState
Subscriber Expiration Info	DisplayString	N/A	R	subExpiration
Inactivity Logoff Timer	DisplayString	N/A	R	subIdleTimeout
Subscriber MBytes Sent	Integer	N/A	R	subBytesSentInMegaByte
Subscriber MBytes Received	Integer	N/A	R	subBytesRecInMegaByte
Total MBytes Sent and Received	Integer	N/A	R	subBytesTotalInMegaByte
Subscriber Proxy Status	DisplayString	N/A	R	subProxy
Subscriber Status	RowStatus	active (1), notInService (2), notReady (3), createAndGo (4), createAndWait (5), destroy (6)	RW	subStatus

Using the Command Line Interface

Miscellaneous Parameters

Name	Type	Values	Access	CLI Parameter
Miscellaneous	Group	N/A	R	misc
Partner Image Splash Screen	Integer	disable (0) enable (1)	RW/Reboot	partnerImageOn
Partner Image Filename	DisplayString Size(1..32)	User Defined	RW/Reboot	partnerImageFileName
Maximum Subscribers Allowed	Integer	N/A	R	maxNumSubscribers
Enable PPTP	Integer	disable (0) enable (1)	RW/Reboot	pptpOn
PPTP Session Idle Timeout	Integer	User Defined	RW/Reboot	pptpIdleTimeout
Enable IPSec	Integer	disable (0) enable (1)	RW/Reboot	ipsecOn

CLI Monitoring Parameters

Using the "show" command with the following table parameters will display operating statistics for the AP-2500 (these are the same statistics that are described in [Monitor Information](#) for the HTTP Web interface).

- **staticmp.** Displays the ICMP Statistics.
- **statarptbl.** Displays the IP ARP Table Statistics.
- **statbridgetbl.** Displays the Learn Table.
- **statif.** Displays information and statistics about the Ethernet and wireless interfaces.
- **stat802.11.** Displays additional statistics for the wireless interfaces.
- **statethernet.** Displays additional statistics for the Ethernet interface.
- **datSessionTable.** Displays the Dynamic Address Translation (DAT) table.

B

XML Interface Specification

This specification describes the AP-2500's XML Interface. Before reviewing this specification, note the following:

- This specification refers to sample HTML files written in JavaScript that illustrate the XML commands (they build an XML object that is sent to the AP). These files are included on the installation CD in the *Docs/samples/* folder.
 - To use the sample files, open each one with a text editor (such as Notepad) and change the **APIPADDR** variable to match your AP's IP address in the following statement:
var usgAddr = "http://APIPADDR:1111/usg/command.xml"
 - Before using the sample files, confirm that the **XML Interface** is enabled and the **XML Sender IP Address** equals the IP address of the computer from which you will send the XML commands (these parameters are located in the **PublicSpace > AAA > Basic** screen).
 - Within the sample files, the term **USG** is synonymous with **AP**.
 - These sample files can only be run from the AP's Ethernet side; you can **not** use these files on a wireless client (subscriber).
 - These sample files are provided for illustration and testing purposes only. Proxim provides no guarantee that these files will function error-free.
- This specification makes reference to a **PMS** billing system and room numbers. These features are not supported by the AP-2500 at this time.

This specification covers the following topics:

- [AP-2500 XML Communication Overview](#)
- [XML Query String Command Format](#)
- [XML Response Form Format](#)
- [AP Command Reference](#)
- [External Authentication Procedure \(Detailed\)](#)

AP-2500 XML Communication Overview

The AP uses XML (eXtensible Markup Language) to communicate with a network device and obtain information about current users. XML is a newer, more elegant way to use custom web content. XML is an open standard that is tied closely into the HTML standard. XML is maintained by the World Wide Web Consortium (W3C). See <http://www.w3.org/> for more information on W3C and XML. Also, see RFC 3470 at <http://www.rfc-editor.org/>.

The XML interface allows the AP to accept and process XML commands from an external source. XML commands are sent from the external device in the form of an encoded query string. The AP parses the query string, executes the commands specified by the string, and returns data to the system that initiated the command request.



NOTE

You can use XML commands with either Internal (IWS) or External (EWS) authentication. You must use XML for EWS authentication; it is optional for IWS authentication.

XML Interface Specification

URL GET

A network device can send commands to the AP via a query string appended to a URL line (GET method). The query string is the string of characters following the question mark (?) at the end of the URL. For example, consider the following example illustrating a "user successful login" command:

http://(AP_IP_ADDR)/userok.htm?UI=(AP_ID)&AC=1&MA=(USER_MAC_ADDR)&ET=(EXP_TIME)&F1=(USER_NAME)&F2=(USER_PW)&CN=(AUTH_CONF_NUM)&SC=(SECURITY_CODE)

userok.htm is a virtual file name that indicates to the AP that the query string contains data about a new user that has been authenticated and should be given access. The parameters are specified using the standard HTML GET method (query string parameter passing).

XML POST

In addition to the HTML GET method, the AP-2500 also supports XML POST commands. There are some similarities between the two methods; both will specify a virtual file name and both will pass parameters within the query string. The differences are in how the commands are encoded within the query string and that with XML the AP will return data to the system that initiated the command request.

Upon receive of an XML POST command, the AP will parse the query string, execute the command specified, and return requested data and/or error response codes in the format of an XML form as part of an HTTP response data stream. An example follows:

HTTP/1.1 200 OK	(specifies request understood)
Server: UI 3A4B6D	(use the AP's ID as the server name)
Date: Fri, 23 Jul 1999 00:09:55 GMT	(current date/time)
Content-Type: text/xml	(specifies XML content)
Last-Modified: Fri, 23 Jul 1999 00:09:55 GMT	(current date/time)
Content-Length: 560	(size of message body in characters)
	(this must be a blank line)
(series of XML tag/data pairs)	
	(end of message body)



NOTE

Refer to the HTTP/1.1 specifications for information of the proper formatting of a HTTP response stream. See <http://www.w3.org/> for details.

XML Query String Command Format

All commands to the AP will be sent using the form POST. The command text will be in the following XML format:

```
<USG COMMAND="(command)" [(attr)="(attr_data)"]>
  <(tag_n) [tag_n_attr = "(tag_n_attr_data)"]>(data_n)</(tag_n)>
</USG>
```

where:

(**command**) is an AP command. Commands are listed later in this specification.

(**attr**) is an optional attribute associated with a command.

(**attr_data**) is the data associated with the optional attribute tag.

(**tag_n**) is a data name tag used for specifying command parameter names.

(**tag_n_attr**) is an optional attribute name tag.

(**tag_n_attr_data**) is optional attribute data.

(**data_n**) is the data associated with a data name tag.



NOTE

The above example contains CRLFs and spacing for display clarity only. A query string must not contain any formatting or line-break characters. It also must be URL encoded.

XML Interface Specification

XML Response Form Format

In response to a command, the AP returns an XML form in the following format:

```
<USG RESULT="(RESULTCODE)" ID="(UI)" IP="(AP_IP_ADDR)">
  [<ERROR_NUM>(error number)</ERROR_NUM>]
  [<ERROR_DESC>(error description)</ERROR_DESC>]
  <(tag_n) [tag_n_attr = "tag_n_attr_data"]>(data_n)</(tag_n)>
</USG>
```

where:

(**RESULTCODE**) is either "OK" or "ERROR".

(**UI**) is the AP ID.

(**AP_IP_ADDR**) is the AP's IP address.

(**tag_n**) is a data name tag.

(**tag_n_attr**) is an optional attribute name tag.

(**tag_n_attr_data**) is optional attribute data.

(**data_n**) is the data associated with a data name tag.

ERROR_NUM and **ERROR_DESC**, see [Response Form Error Codes](#).

The number of tag/data pairs in the query string and return form will vary depending on the parameters required for the command and the data returned by the command. See [AP Command Reference](#).

Response Form Error Codes

All response forms returned after a command request will always contain error information. The attribute **RESULT** will be assigned either "OK" or "ERROR." If an error did occur, two additional tag/data pairs will be added as part of the response form: **ERROR_NUM** and **ERROR_DESC**. The error number data will contain an integer number representing the error that occurred. The error description data will be a readable text description of the error.

The following is a list of error codes:

Error No.	Error Description String
100	Parsing error
101	Unrecognized command
102	Required attribute is missing
103	Required data is missing
200	Unknown room number
201	Unknown user name
202	Unknown user MAC address
203	Incorrect password
204	Username already present
205	Too many subscribers
206	Unable to provide all requested data
207	AAA internal error
300	User RADIUS account not found
301	User RADIUS authorization denied
302	User PMS authorization denied
303	Unsupported payment method

AP Command Reference

Add/Update User

Sample file name: **UserAdd.htm**

The specified user has been authorized for access and will be added to the AP's Authorized Subscribers Table.

Command:	"USER_ADD"
Command attr:	"MAC_ADDR"
Command attr_data:	user MAC address (string)
tag_1:	"USER_NAME"
data_1:	(user name)
tag_2:	"PASSWORD"
tag_2_attr:	"ENCRYPT"
tag_2_attr_data:	"TRUE" or "FALSE"
data_2:	(user password)
tag_3:	"EXPIRY_TIME"
tag_3_attr:	"UNITS"
tag_3_attr_data:	"SECONDS" , "HOURS" , "DAYS"
data_3:	(number of expiry units)
tag_4:	"ROOM_NUMBER"
data_4:	(user's room number)
tag_5:	"PAYMENT_METHOD"
data_5:	"RADIUS" , "PMS" , "CREDIT_CARD" , or "ROOM_OPEN"
tag_6:	"CONFIRMATION"
data_6:	(confirmation code/ID)
tag_7:	"PAYMENT"
data_7:	(amount paid for access)

Returns: Standard response form

Update Cache

Sample file name: **UpdateCache.htm**

The user's status in the Current Subscribers Table will change from "Pending" to "Valid".



NOTE

It is important to update the cache to enable proper access for the user.

Command:	"CACHE_UPDATE"
Command attr:	"MAC_ADDR"
Command attr_data:	User MAC address (string)
tag_1:	"PAYMENT_METHOD"
data_1:	"RADIUS" , "PMS" , "CREDIT_CARD" , or "ROOM_OPEN"

Returns: Standard response form

XML Interface Specification

Bandwidth Up

Set the bandwidth up for an authorized user.

Command: **"SET_BANDWIDTH_UP"**
Command attr: **"SUBSCRIBER"**
Command attr_data: User MAC address (string)
tag_1: **"BANDWIDTH_UP"**
data_1: (number measured in Kbps (i.e. for 128,000 bit per second, enter 128))

Returns: Standard response form

Bandwidth Down

Set the bandwidth down for an authorized user.

Command: **"SET_BANDWIDTH_DOWN"**
Command attr: **"SUBSCRIBER"**
Command attr_data: User MAC address (string)
tag_1: **"BANDWIDTH_DOWN"**
data_1: (number measured in Kbps (i.e. for 128,000 bit per second, enter 128))

Returns: Standard response form

Delete User

Sample file name: **UserDelete.htm**

The User will be deleted (based on MAC address or user name).

Command: **"USER_DELETE"**
tag_1: **"USER"**
tag_1_attr: **"ID_TYPE"**
tag_1_attr_data: **"MAC_ADDR"** or **"USER_NAME"**
data_1: if **ID_TYPE = "MAC_ADDR"** then (User's MAC address)
if **ID_TYPE = "USER_NAME"** then (user name)

Returns: Standard response form

XML Interface Specification

Query User

Sample file name: **UserQuery.htm**

The current User data is returned.

Command: **"USER_QUERY"**
tag_1: **"USER"**
tag_1_attr: **"ID_TYPE"**
tag_1_attr_data: **"MAC_ADDR" or "USER_NAME"**
data_1: if **ID_TYPE = "MAC_ADDR"** then (User's MAC address)
if **ID_TYPE = "USER_NAME"** then (user name)

Returns: Standard response form
tag_1: **= "MAC_ADDR"**
data_1: **= (User's MAC address)**
tag_2: **= "USER_NAME"**
data_2: **= (user name)**
tag_3: **= "PASSWORD"**
data_3: **= (User's password)**
tag_4: **= "EXPIRY_TIME"**
tag_4_attr: **= "UNITS"**
tag_4_attr_data: **= "SECONDS", "HOURS", "DAYS"**
data_4: **= (number of expiry units)**
tag_5: **= "ROOM_NUMBER"**
data_5: **= (User's room number)**
tag_6: **= "PAYMENT_METHOD"**
data_6: **= "RADIUS", "PMS", "CREDIT_CARD", "ROOM"**
tag_7: **= "DATA_VOLUME"**
data_7: **= (data transferred by User in Kbytes)**

Authorize User

A User's identity, specified by MAC address, is checked against the Authorized Subscribers and Current Subscribers Tables. If the User is found in either table, **VALID_USER** is returned along with the User's authorization method: **RADIUS**, **PMS** (not supported), **CREDIT_CARD**, or **ROOM** (not supported). If the User is not found, **INVALID_USER** will be returned.

Command: **"USER_AUTHORIZE"**
Command attr: **"MAC_ADDR"**
Command attr_data: User MAC address (string)

Returns: Standard response form
tag_1: **= "STATUS"**
data_1: **= "VALID_USER" or "INVALID_USER"**
tag_2: **= "PAYMENT_METHOD"**
data_2: **= "RADIUS", "PMS", "CREDIT_CARD", or "ROOM"**

XML Interface Specification

Commands For Reference Only

The following commands are included for reference purposes only. They are not currently supported by the AP-2500.

Set Room Access

The specified room access mode is set.

Command: **"ROOM_SET_ACCESS"**
Command attr: **"ROOM_NUMBER"**
Command attr_data: Room number (8 char. max string)
tag_1: **"ACCESS_MODE"**
data_1: **"ROOM_OPEN", "ROOM_CHARGE", or "ROOM_BLOCK"**

Returns: Standard response form

Query Room Status

The specified room access mode is returned.

Command: **"ROOM_QUERY_ACCESS"**
Command attr: **"ROOM_NUMBER"**
Command attr_data: Room number (8 char. max string)

Returns: Standard response form
tag_1 = **"ROOM_NUMBER"**
data_1 = (room number)
tag_2 = **"ACCESS_MODE"**
data_2 = (room access mode)

Where: room access mode = **"ROOM_OPEN", "ROOM_CHARGE", or "ROOM_BLOCK"**

User Purchase

A user e-commerce or special service purchase is to be charged. Currently, the only option is to charge the user's bill via the PMS system.

Command: **"USER_PURCHASE"**
Command attr: **"ROOM_NUMBER"**
Command attr_data: (room number)
tag_1: **"ITEM_CODE"**
data_1: (item code)
tag_2: **"ITEM_DESCRIPTION"**
data_2: (description of purchase)
tag_3: **"ITEM_AMOUNT"**
data_3: (amount of item with out tax)
tag_4: **"ITEM_TAX"**
data_4: (tax charged on item)
tag_5: **"ITEM_TOTAL"**
data_5: (total amount charged including tax)

Returns: Standard response form

XML Interface Specification

User Payment

User's authorization and payment is requested. PMS is not supported by the AP at this time.

Command:	"USER_PAYMENT"
Command attr:	"PAYMENT_METHOD"
Command attr_data:	"PMS"
tag_1:	"USER_NAME"
data_1:	(user name)
tag_2:	"PASSWORD"
tag_2_attr:	"ENCRYPT"
tag_2_attr_data:	"TRUE" or "FALSE"
data_2:	(user password)
tag_3:	"EXPIRY_TIME"
tag_3_attr:	"UNITS"
tag_3_attr_data:	"SECONDS" , "HOURS" , "DAYS"
data_3:	(number of expiry units)
tag_4:	"ROOM_NUMBER"
data_4:	(user's room number)
tag_5:	"PAYMENT"
data_5:	(amount charged for access)
Returns:	Standard response form
tag_1:	= "CONFIRMATION"
data_1:	= (confirmation number/ID)

➤ NOTE

If you are not requiring users to enter User Names, then auto-set the USER_NAME when doing the USER_ADD command to the user's MAC address and import the MAC address to data_1.

External Authentication Procedure (Detailed)

Whenever a subscriber tries to access the Internet, it must pass through the AP. The AP tracks all packets flowing through it by the source MAC address of the packet, which uniquely identifies the wireless card that the subscriber is using. If the MAC address is already in the AP's Authorized Subscribers Table, the AP will check the expiration time to see if the user is able to access the Internet.

If the MAC address is not known, the AP automatically redirects all Web page requests from the subscriber to the Login page stored on the External Web Server and passes several parameters to identify the subscriber and the AP. This section defines the format of the URL redirect the AP and External Web Server must support in order to provide a seamless Web page-based subscription signup process for the new subscriber. When the AP is configured for an EWS, the EWS is responsible for interacting with accounting or authorizing services.

⇒ NOTE

The following procedure is an in-depth look at the communication process between the AP and an EWS when authenticating a user. It describes the same procedure as [External Authentication > Authentication Procedure](#) but in greater detail. Examples for each numbered item below can be found in [Sample XML Communications with the AP](#).

1. When a new subscriber opens his/her Web browser, the AP accepts the TCP connection and gets the original Web Page Request from the subscriber. This URL is stored as the Origin Server (OS). The AP generates a META Redirect, which causes the subscriber to automatically close the TCP connection with the AP and the Subscriber will connect directly to the EWS (as configure by the administrator in the AP). Also, using the HTML GET method, the AP displays the subscriber's information in the URL line (such as the MAC address, etc.).

Example:

http://EWS_IP_ADDR/usg/newuserlogin.asp?UI=000450&UURL=http://AP_IP_ADDR/userok.htm&MA=0010A4B732BB&RN=&OS=http://204.71.200.68&SC=18056

2. The EWS using the HTTP POST method sends the **USER_ADD** command to the AP with the MAC address (captured from step #1), the User Name/Password (entered by user), Expiration Time (in seconds), Payment Method, and Payment (payment amount).
3. The AP now using the HTTP POST method sends a reply indicating that it has received the command and has executed it. (The AP adds the new user to the Authorized Subscribers Table.)

⇒ NOTE

The AP will send the reply to the original sender and only if that sender is located on the same server that has been specified as the **XML Sender IP Address** in the AP's **PublicSpace > AAA > Basic** screen.

4. The EWS using the HTTP POST method sends the **CACHE_UPDATE** command to the AP with the MAC address (captured from step #1).
5. The AP using the HTTP POST method sends a reply indicating that it has received the command and has executed it. (The AP updates the user's State from Pending to Valid in the Current Subscribers Table.)
6. The EWS using the HTTP POST method sends the **SET_BANDWIDTH_UP** with the Bandwidth-Up parameter.
7. The AP using the HTTP POST method sends a reply indicating that it has received the command and has executed it.
8. The EWS using the HTTP POST method sends the **SET_BANDWIDTH_DOWN** with the Bandwidth-Down parameter.
9. The AP using the HTTP POST method sends a reply indicating that it has received the command and has executed it.

Definition of parsed parameters the AP sends over the URL line (GET method):

- **UI:** The globally unique ID of the AP. The maximum length is 6 characters. It is actually the last 6 characters of the AP's public Ethernet port MAC address.
- **UURL:** The URL on the AP to which the EWS should redirect the subscriber following successful Authorization.
- **MA:** The unique MAC Address of the subscriber's Network Interface Card used to identify that subscriber.
- **RN:** Identifies the room number. This feature is not currently support so RN will be blank.
- **OS:** The Origin Server URL. This is the URL originally requested by the subscriber.
- **SC:** A Security Code used as a key to generate the SC for the External Web Server when used with a credit card clearing house; this parameter is not used when the AP is configured to communicate with an EWS over XML.

Sample XML Communications with the AP

The following is an example of the commands to set access for a new subscriber with the following attributes:

User Name: johndoe

MAC address: 0050da554787

NOTE

The following examples contain CRLFs and spacing for display clarity only. A query string must not contain any formatting or line-break characters. It also must be URL encoded.

1. AP sends (via HTML GET Method to `http://[Your Server IP Address]/[Your Scripts]`):
`http://[Your Server IP Address]/[Your Scripts]?UI=000177&UURL=http://208.46.165.157&MA=0050da554787&RN=101&OS=http://204.71.200.74&SC=6302`
2. EWS sends (via HTTP POST Method to `http://[AP_IP_Address]:1111/usg/command.xml`):
**`<USG COMMAND="USER_ADD" MAC_ADDR="0050da554787">
<USER_NAME>johndoe</USER_NAME>
<PASSWORD ENCRYPT="FALSE">doededoe</PASSWORD>
<EXPIRY_TIME UNITS="SECONDS">3600</EXPIRY_TIME>
<ROOM_NUMBER></ROOM_NUMBER>
<PAYMENT_METHOD>RADIUS</PAYMENT_METHOD>
<CONFIRMATION></CONFIRMATION>
<PAYMENT></PAYMENT>
</USG>`**
3. AP sends (via HTTP POST Method to `http://[Your Server IP Address]/[Your Scripts]`):
`<USG RESULT="OK" ID="00011B" IP="208.46.165.30"></USG>`
Where: the ID is the AP's ID and the IP is the AP's IP address.
4. EWS sends (via HTTP POST Method to `http://[AP_IP_Address]:1111/usg/command.xml`):
**`<USG COMMAND="CACHE_UPDATE" MAC_ADDR="0050da554787">
<PAYMENT_METHOD>RADIUS</PAYMENT_METHOD>
</USG>`**
5. AP sends (via HTTP POST Method to `http://[Your Server IP Address]/[Your Scripts]`):
`<USG RESULT="OK" ID="00011B" IP="208.46.165.30"></USG>`
6. EWS sends (via HTTP POST Method to `http://[AP_IP_Address]:1111/usg/command.xml`):
**`<USG COMMAND="SET_BANDWIDTH_UP" SUBSCRIBER="0050da554787">
<BANDWIDTH_UP>3000</BANDWIDTH_UP>
</USG>`**
7. AP sends (via HTTP POST Method to `http://[Your Server IP Address]/[Your Scripts]`):
`<USG RESULT="OK" ID="00011B" IP="208.46.165.30"></USG>`
8. EWS sends (via HTTP POST Method to `http://[AP_IP_Address]:1111/usg/command.xml`):
**`<USG COMMAND="SET_BANDWIDTH_DOWN" SUBSCRIBER="0050da554787">
<BANDWIDTH_DOWN>1500</BANDWIDTH_DOWN>
</USG>`**
9. AP Sends (via HTTP POST Method to `http://[Your Server IP Address]/[Your Scripts]`):
`<USG RESULT="OK" ID="00011B" IP="208.46.165.30"></USG>`

Credit Card Interface Specification

A key payment feature of the AP-2500 is direct Credit Card billing. The AP supports several credit card service companies by default (see [Credit Card Services](#)). However, if your particular credit card service provider or clearinghouse is not supported by default, you can provide the following specification to your clearinghouse. Note that your clearinghouse will need to develop an interface for their system to communicate with the AP; this specification should provide them with the information they need to create the interface.



CAUTION

This is a “best effort” specification. Proxim cannot guarantee that following these guidelines will ensure trouble-free interoperability between the credit card clearing server and the AP-2500.

Data sent by the AP-2500 to the credit card clearing server



NOTE

This example uses US dollars as the currency, but the AP-2500 supports any currency.

```

1 <input type=hidden name=FNAME value=%d">\n" :
2 <input type=hidden name=MA value=%s">\n" :
3 <input type=hidden name=IP value=%lu">\n" :
4 <input type=hidden name=servidx value=%d">\n" :
5 <input type=hidden name=OS value=%s">\n" :
6 <input type=hidden name=PAID value=%s">\n" :
7 <input type=hidden name=timeUnit value=%s">\n"), :
8 <input type=hidden name=x_Login value=%s">\n" :
9 <input type=hidden name=x_Amount value=%s">\n" :
10 <input type=hidden name=x_ADC_URL value=http://%s:%d/usg/silent">\n":
11 <input type=hidden name=x_ADC_Relay_Response value=TRUE">\n"
12 <input type=hidden name=x_Show_Form value=PAYMENT_FORM">\n"
13 <input type=hidden name=x_Test_Request value=FALSE">\n"
14 <input type=hidden name=x_Color_Background value=%s">\n"
15 <input type=hidden name=x_Description value=Purchasing %s Internet access">\n":
16 <input type=hidden name=x_Cust_ID value=%s-%s">\n" :
17 <input type=hidden name=UN value=%s">\n" :
18 <input type=hidden name=UI value=%s">\n"), :
```

Explanation:

1. Form name
2. Subscriber's MAC address
3. IP address of the subscriber
4. Internal plan number
5. Originating server
6. Amount paid
7. Time unit (for example, day or hour)

Credit Card Interface Specification

8. Merchant ID
9. Amount
10. URL to post silent reply
11. This field must be in the form and set to a value of TRUE to tell the system that it will be doing an ADC Relay Response transaction.
12. Sending this field guarantees that the default Payment Form will show up for the user. Should be VALUE="PAYMENT_FORM" to show default.
13. If an account is not in Test Mode, and it is necessary to perform a test on a single transaction, it is possible to send the x_Test_Request="TRUE" field as part of the transaction. Sending this field set to TRUE overrides the setting of Test Mode in the merchant's settings, and invokes Test Mode for the particular transaction with which the field is sent. Note that if Test Mode is turned on in a merchant's settings, that setting can't be overridden by sending x_Test_Request="FALSE".
14. Any valid HTML color name or color hex code sent in this field will set that color as the background color for both the Payment Form and the Receipt Page.
15. Plan name description
16. Customer ID; it is in the form of AP's ID-SUBSCRIBER MAC.
17. User name
18. AP's ID

Data sent by credit card clearing server to the AP-2500

The following items need to be posted to the silent URL of the AP-2500:

- 1 x_amount = websGetVarIgnoreCase(wp, T("x_amount"), T("0"));
- 2 x_trans_id = websGetVarIgnoreCase(wp, T("x_trans_id"), T("0"));
- 3 x_response_code = websGetVarIgnoreCase(wp, T("x_response_code"), T("0"));
- 4 x_response_reason_text = websGetVarIgnoreCase(wp, T("x_response_reason_text"), T("0"));
- 5 UI = websGetVarIgnoreCase(wp, T("UI"), T("defaultData"));
- 6 servidx = atoi(websGetVarIgnoreCase(wp, T("servidx"), T("0")));
- 7 MA = websGetVarIgnoreCase(wp, T("MA"), T("defaultData"));
- 8 IP = websGetVarIgnoreCase(wp, T("IP"), T("0"));
- 9 UN = websGetVarIgnoreCase(wp, T("UN"), T(""));
- 10 OSP = websGetVarIgnoreCase(wp, T("OS"), T(""));

Explanation:

1. Amount
2. This number identifies the transaction in the system, and can be used to submit a modification of this transaction at a later time via HTTP(S) form POST (such as voiding the transaction, or capturing an Auth Only transaction).
3. Response_code = 1 (1= transaction accepted)



NOTE

NOTE: The AP only cares if the response code = 1, in all other cases, we assume the transaction is not accepted. There are different codes for different failures. For e.g., code = 3 is for Invalid Credit card number.

4. Example: This transaction has been approved
5. AP's ID
6. This an echo of the internal plan number that the AP passes.
7. MAC address of user
8. IP address of user
9. User Name of user
10. Originating Server

D

ASCII Character Chart

You can configure WEP Encryption Keys in either Hexadecimal or ASCII format. Hexadecimal digits are 0-9 and A-F (not case sensitive). ASCII characters are 0-9, A-F, a-f (case sensitive), and punctuation marks. Each ASCII character corresponds to two hexadecimal digits.

The table below lists the ASCII characters that you can use to configure WEP Encryption Keys. It also lists the Hexadecimal equivalent for each ASCII character.

ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent
!	21	9	39	Q	51	i	69
"	22	:	3A	R	52	j	6A
#	23	;	3B	S	53	k	6B
\$	24	<	3C	T	54	l	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
'	27	?	3F	W	57	o	6F
(28	@	40	X	58	p	70
)	29	A	41	Y	59	q	71
*	2A	B	42	Z	5A	r	72
+	2B	C	43	[5B	s	73
,	2C	D	44	\	5C	t	74
-	2D	E	45]	5D	u	75
.	2E	F	46	^	5E	v	76
/	2F	G	47	_	5F	w	77
0	30	H	48	`	60	x	78
1	31	I	49	a	61	y	79
2	32	J	4A	b	62	z	7A
3	33	K	4B	c	63	{	7B
4	34	L	4C	d	64		7C
5	35	M	4D	e	65	}	7D
6	36	N	4E	f	66	~	7E
7	37	O	4F	g	67		
8	38	P	50	h	68		

Specifications

In This Chapter

- [Hardware Specifications](#)
- [Radio Specifications](#)
 - [802.11b Channel Frequencies](#)
 - [802.11a Channel Frequencies](#)
 - [Wireless Communication Range](#)

Hardware Specifications

Physical Specifications

AP-2500 Unit

Dimensions (H x W x L) = 6.5 x 18.5 x 26 cm (2.5 x 7.25 x 10.25 in.)
Weight = 1.75 kg (3.5 lb.)

802.11a Antenna Adapter

Dimensions (H x W x L) = 11.3 x 2.10 x 26.2 cm (4.5 x 0.83 x 10.3in.)
Weight = 0.18 kg (0.4 lb.)

Electrical Specifications

Without Active Ethernet Module

Voltage = 100 to 240 VAC (50-60 Hz)
Current = 0.2 amp
Power Consumption = 20 Watts

With Active Ethernet Module

Input Voltage = 42 to 60 VDC
Output Current = 200mA at 48V
Power Consumption = 9-10 Watts

Environmental Specifications

AP-2500 Unit

Operating = 0° to 40°C (32° to 104 °F) @ 20 to 90% relative humidity
Transport = -40° to 60°C (-40° to 140°F) @ 15 to 95% relative humidity (no condensation allowed)
Storage = -10° to 60°C (14° to 140°F) @ 10 to 90% relative humidity (no condensation allowed)

802.11a Antenna Adapter

Operating = 0° to 70°C (32° to 158 °F) @ 20 to 90% relative humidity
Transport = -40° to 75°C (-40° to 167 °F) @ 15 to 95% relative humidity
Storage = -20° to 75°C (-4° to 167 °F) @ 10 to 95% relative humidity

Specifications

Ethernet Interface

10/100 Base-T, RJ-45 female socket

PCMCIA Interface

PC Card Slot (A & B) = Standard PC Card slot for PC Card

Serial Port Interface

Connector Type = DB9, male

Serial Cable = Standard RS-232C serial data cable, with a female DB-9 connector at each end

Active Ethernet Interface

Category 5, foiled, twisted pair cables must be used to ensure compliance with FCC Part 15, subpart B, Class B requirements

Standard 802.3af pin assignments

HTTP Interface

Microsoft Internet Explorer 5.5 or better (preferred), or Netscape 6 or higher.

Radio Specifications

802.11a radio certification is not available in all countries. Contact your sales representative for details.

802.11b radio certification is available in the US/Canada (FCC), Japan (VCCI), Europe (ETSI), and France.

802.11b Channel Frequencies

The following table shows the channel allocations that vary from country to country. Values listed in bold font indicate default channels and frequencies.

Channel ID	FCC/World (MHz)	ETSI (MHz)	France (MHz)	Japan (MHz)
1	2412	2412	-	2412
2	2417	2417	-	2417
3 (default - most countries)	2422	2422	-	2422
4	2427	2427	-	2427
5	2432	2432	-	2432
6	2437	2437	-	2437
7	2442	2442	-	2442
8	2447	2447	-	2447
9	2452	2452	-	2452
10	2457	2457	2457	2457
11 (default-France)	2462	2462	2462	2462
12	-	2467	2467	2467
13	-	2472	2472	2472
14				2484

Table E-1 802.11b Channel Frequencies

802.11a Channel Frequencies

The following table shows the channel allocations that vary from country to country. Values listed in bold font indicate default channels and frequencies.

Channel ID	FCC/World (MHz)	ETSI (MHz)	Japan (MHz)
34	-	-	5170
36	5180	5180	-
38	-	-	5190
40	5200	5200	-
42	-	-	5210
44	5220	5220	-
46	-	-	5230
48	5240	5240	-
52	5260	5260	-
56	5280	5280	-
60	5300	5300	-
64	5320	5320	-

Table E-2 802.11a Channel Frequencies

Specifications

Wireless Communication Range

The range of the wireless signal is related to the composition of objects in the radio wave path, and the transmit rate of the wireless communication. Communications at a lower transmit range may travel longer distances.

NOTE

The range values listed in the Communications Range Chart are typical distances as measured at the development laboratories. These values provide a rule of thumb and may vary according to the actual radio conditions at the location where the product is used.

The range of your wireless devices can be affected when the antennas are placed near metal surfaces and solid high-density materials. Ranges for outdoor antenna installations are related to type of outdoor antennas used, and length of antenna cables. Range is also impacted due to “obstacles” in the signal path of the radio that may either absorb or reflect the radio signal.

In Open Office environments, antennas can “see” each other (no physical obstructions between them). In Semi-open Office environments, workspace is divided by shoulder-height, hollow wall elements; antennas are at desktop level. In a Closed Office environment, solid walls and other obstructions may affect signal strength.

The following tables show typical range values for various environments.

Range	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Open Office	160 m (525 ft.)	270 m (885 ft.)	400 m (1300 ft.)	550 m (1750 ft.)
Semi-Open Office	50 m (165 ft.)	70 m (230 ft.)	90 m (300 ft.)	115 m (375 ft.)
Closed Office	25 m (80 ft.)	35 m (115 ft.)	40 m (130 ft.)	50 m (165 ft.)
Receiver Sensitivity	-82 dBm	-87 dBm	-91 dBm	-94 dBm
Delay Spread (at FER of <1%)	65 ns	225 ns	400 ns	500 ns

Table E-3 802.11b Wireless communication ranges

Range	54 Mbps	48 Mbps	36 Mbps	24 Mbps	18 Mbps	12 Mbps	9 Mbps	6 Mbps
Open Office	19 m (62 ft.)	35 m (115 ft.)	74 m (243 ft.)	112 m (367 ft.)	153 m (502 ft.)	189 m (620 ft.)	232 m (761 ft.)	258 m (846 ft.)
Semi-Open Office	17 m (56 ft.)	29 m (95 ft.)	34 m (111 ft.)	49 m (161 ft.)	63 m (206 ft.)	76 m (249 ft.)	90 m (295 ft.)	99 m (325 ft.)
Closed Office	15 m (49 ft.)	24 m (79 ft.)	27 m (88 ft.)	36 m (118 ft.)	45 m (147 ft.)	52 m (170 ft.)	60 m (197 ft.)	64 m (210 ft.)
Receiver Sensitivity	-65 dBm	-69 dBm	-73 dBm	-77 dBm	-80 dBm	-82 dBm	-84 dBm	-85 dBm

Table E-4 802.11a Wireless communication ranges

Technical Support

If you are having a problem using an AP-2500 and cannot resolve it with the information in [Troubleshooting](#), gather the following information and contact your local authorized reseller.

Gather the following information before contacting your reseller:

- List of ORiNOCO products installed on your network; include the following:
 - Product names and quantity
 - Part numbers (P/N)
 - Serial numbers (S/N)
- List of ORiNOCO software versions installed
 - For the AP-2500, check the Web browser interface's [Version](#) screen
 - Include the source of the software version (e.g., pre-loaded on unit, installed from CD, downloaded from Proxim Web site, etc.)
- Information about your network
 - Network operating system (e.g., Microsoft Networking); include version information
 - Protocols used by network (e.g., TCP/IP, NetBEUI, IPX/SPX, AppleTalk)
 - Ethernet frame type (e.g., 802.3, Ethernet II), if known
 - IP addressing scheme (include address range and whether static or DHCP)
 - Network speed and duplex (10 or 100 Mbits/sec; full or half duplex)
 - Type of Ethernet device that the Access Points are connected to (e.g., Active Ethernet power injector, hub, switch, etc.)
 - Type of Security enabled on the wireless network (None, WEP Encryption)
- A description of the problem you are experiencing
 - What were you doing when the error occurred?
 - What error message did you see?
 - Can you reproduce the problem?
 - For each ORiNOCO product, describe the behavior of the device's LEDs when the problem occurs



NOTE

The latest software and documentation is available for download at <http://www.proxim.com/>.

If necessary, you can contact Proxim Technical Support directly. However, all queries should first be directed to your local supplier.

- All Customers are entitled to have 30 days free customer support. Please note that all Support Requests which are outside of the 30-day free support time will be charged a fee of \$25.00 (US Dollars) per incident.
- Authorized partners are entitled to have unlimited customer support.
- To receive e-mail technical support, please include the serial number of the product(s) in question. The serial number should be on the product and conform to the following format: ##UT##### or ##R7#####. We will be unable to respond to your inquiry without this information.

For the U.S. and Canada:

Phone: 1-866-ORiNOCO (1-866-674-6626)
E-mail: USAsupport@orinocowireless.com

Technical Support



For the Caribbean and Latin America:

Phone: 1-866-ORiNOCO (1-866-674-6626)
1-661-367-2230

E-mail: CALAsupport@orinocowireless.com

For Asia Pacific:

Phone: +1 661-367-2230

E-mail: APACsupport@orinocowireless.com

For Europe, the Middle East, and Africa (EMEA):

Your local supplier in the EMEA region is trained to give you the support you require. Local suppliers have direct access to the ORiNOCO Technical Support Center and will help you in every way they can.

Phone: +1 661-367-2230

E-mail: EMEAsupport@orinocowireless.com